DOMESTIC INFORMATION WARFARE: THE DEPARTMENT OF DEFENSE'S ROLE IN THE CIVIL DEFENSE OF THE NATIONAL INFORMATION INFRASTRUCTURE

A MONOGRAPH
BY
Major Ted T. Uchida
U.S. Air Force

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

Second Term AY 97-98

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	21 May 1998	Monograph

4. TITLE AND SUBTITLE
Domestic Information Warfare: The Department of Defense's Role in the Civil Defense of the National Information Infrastructure

5. FUNDING NUMBERS

6. AUTHOR(S)
MAJ TED T. UCHIDA

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
School of Advanced Military Studies
Command and General Staff College
Fort Leavenworth, Kansas 66027

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Command and General Staff College
Fort Leavenworth, Kansas 66027

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE:
DISTRIBUTION UNLIMITED.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*
SEE ATTACHED

14. SUBJECT TERMS

15. NUMBER OF PAGES
81

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

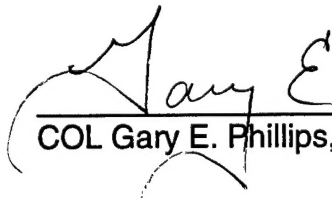
SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

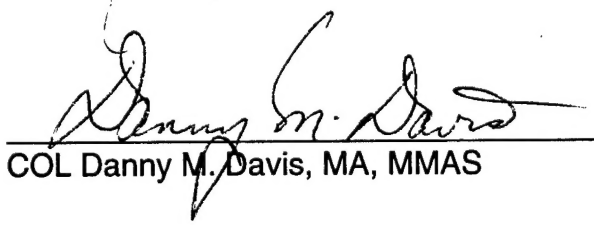
Major Ted T. Uchida

Title of Monograph: *Domestic Information Warfare: The Department of Defense's Role in the Civil Defense of the National Information Infrastructure*

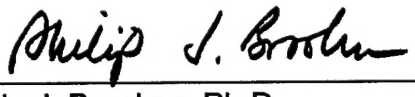
Approved by:



COL Gary E. Phillips, MA — Monograph Director



COL Danny M. Davis, MA, MMAS — Director, School of Advanced Military Studies



Philip J. Brookes, Ph.D. — Director, Graduate Degree Program

Accepted this 21st Day of May 1998

ABSTRACT

Domestic Information Warfare: The Department of Defense's Role in the Civil Defense of the National Information Infrastructure by Major Ted T. Uchida, USAF, pages.

Now more than ever every facet of society relies on the NII to facilitate critical information related activities. Entities around the world have not ignored this transformation and seek to steal, disrupt, and interdict the US's key information processes. It is this reliance on the NII and the security threats it faces that force policy makers to answer the question who should protect the NII? Seemingly, the DoD is well positioned to take the lead role in protecting the NII. However, authorizing DoD control over NII protection ignores many issues.

Analyzing vulnerabilities to the DII illustrates the gravity of the problem the entire NII faces. The DII faces an increasing threat from hackers, and rogue agents bent on damaging the DoD's information based processes. Countering these threats requires developing a comprehensive NII protection strategy. Correspondingly, developing a strategy for protecting the NII requires defining several strategic concepts of Centers of Gravity, objective, end state, and key tasks.

Along with strategic concepts, several critical environmental paradigms such as changing mediums of warfare and the source of future power also effect decisions of who should protect the NII. In light of environmental paradigms and strategic concepts, the issue of whether the DoD can serve as lead agent in NII protection begins to take shape. While arguments such as experience in matters related national security appear to point toward the DoD playing the central role in NII protection, the underlying rationale is limiting and shortsighted. The NII's distributed nature, constitutionally mandated rights, and the needs of a pluralistic society, all argue against the DoD playing a lead role in protecting the NII.

While the DoD should not play the lead role, it does have the capacity to take leadership in several key sub-task areas. First, the DoD should be the lead agent facilitating discussion about national incident and consequence management plans. Second, the DoD should be responsible for protecting a core set of functions related to critical incident and consequence management capabilities. The monograph concludes by recommending the US develop a national campaign plan to protect the NII. This campaign plan should address how deterrence would be used as a strategy, the development of an organization solely dedicated to implementing and managing NII protection plans, and to what extent defense will be the only method utilized to protect the NII.

Table of Contents

Chapter One: Setting the Stage **1**
Introduction 1
Case Study: Intrusion of USAF Rome Laboratories 3
Definitions 5
Proliferation of the Information Infrastructures 6
Attacks on the DII and NII 10
Threats & Vulnerabilities of Information Infrastructures 11
Summary 13
Chapter Two: Elements of Strategy **15**
DII and NII Centers of Gravity 15
Strategic Objectives and End State 21
Elements of Strategy 23
Specified Tasks 26
Summary 27
Chapter Three: Paradigms and the DoD Role **29**
Prologue: Information Age Paradigms 29
Can the DoD Handle the Job Alone? 32
Summary 39
Chapter Four: A Strategy for Protecting the NII **41**
Prevention and Mitigation, an Individual Responsibility 41
Policy Formulation, A Governmental Responsibility 44
Information Sharing, A National Intelligence Responsibility 46
Incident Management and Consequence Management 49
Summary 52
Conclusion **54**
Endnotes **59**
Bibliography **73**

Table of Figures

Figure 1: Number of Attacks Against DoD Computers **10**
Figure 2: Key COG and Critical Vulnerabilities for NII and DII Protection **19**
Figure 3: Information System Protection Choices **25**

Chapter One: Setting the Stage

Introduction

Rapid expansion of computer networks and their application to a litany of military and civilian applications has created a new national infrastructure. This new electronic infrastructure is the backbone upon which much of the US's future economic expansion, global competitiveness, and military power rests. Networks of interconnected computers, which are quickly becoming a vital national interest, allow business, government, and the US Armed Forces to share information, direct operations, and reach new levels of performance. These computers and their connections represent the National Information Infrastructure (NII).

Application of computer networking within the US Armed Forces is also creating a parallel infrastructure called the Defense Information Infrastructure (DII). Inextricably tied to the NII, the DII globally links military functions such as command and control, administration, communication, research and development, and intelligence and targeting.[1] The DII represents a cornerstone for future warfighting doctrine and a vital capability US Armed Forces will rely on in future operations.[2]

While facilitating a rapid growth in efficiency and combat capability, DII expansion creates new opportunities for adversaries bent on destroying, manipulating, and stealing information.[3] Using the DII and its links to the NII, intruders threaten information infrastructures the US Armed Forces rely upon to transfer information, and communicate globally. Furthermore, continuing automation and connection of new processes to the DII only increases nodes intruders can use to steal or corrupt information, damage the United

State's key infrastructures, and create havoc in domestic society. Future trends in technology and doctrine signal that the Department of Defense's (DoD) reliance on the interconnection of the NII and DII will continue increasing vulnerability of US Armed Forces to information-based infrastructure attacks.

The interconnected nature of the DII and NII and the emergence of new threats seemingly requires the DoD to protect both. However, to propose the DoD take on direct responsibility for domestic defense of the NII raises many concerns. The heart of the NII protection issue revolves around whether the DoD has the legal authority and economic ability to actively protect a structure not purely for military use. Areas including privacy, free access, free speech, and the extent to which the DoD can conduct domestic internal defense adds further complexity to the debate. Therefore the central issue of debate is whether DoD should play a central or supporting role in defense of the NII.

Demonstrating whether or not the DoD has the sole responsibility to protect the NII from threats bent on denying, destroying, or corrupting key information infrastructures requires establishing three concepts. First, the NII must be established as a vital national security interest. After establishing the NII as a vital national security interest, the debate next examines the best strategy to protect it from attack. Finally, the DoD can be analyzed to see if it has the capability and resources to protect implement the strategy. Identifying whether the DoD should play a leading role for protection of the NII also requires demonstrating that it structurally possesses the ability to implement required protection, the role for civilian and governmental agencies, and the limits of DoD operations.

Case Study: Intrusion of USAF Rome Laboratories

Studying the details of an Information Warfare (IW) penetration of a military information system illustrates the potential threat the NII faces. The case involved the March 1994 penetration of the USAF's Rome Air Development Center (Rome Labs) computer systems.[4] Rome Labs is the USAF's primary facility dedicated to command and control research. Some of Rome Labs projects include work in artificial intelligence, radar guidance, and target detection and tracking systems.[5]

On 28 March 1994, Rome Labs systems administrators discovered an unauthorized penetration of its computer system. Further investigation by administrators detected the presence of a covertly installed password "sniffer"[6] program. Realizing the severity of the situation, administrators immediately notified the Defense Information Systems Agency (DISA), the Air Force Office of Special Investigations, and the Air Force Information Warfare Center's computer security experts. Each of these agencies, working in concert, discovered the penetration of seven computer systems and 30 sensitive databases by two unknown individuals as early as 23 March 1994, using the Internet. Besides copying sensitive information, the intruders used their unauthorized access to penetrate other systems such as the Goddard Space Flight Center, NATO Headquarters, and the Korean Atomic Research Institute.

While computer security experts detected and monitored unauthorized intrusions, tracing the intruders back to their originating location proved difficult. Employing "keystroke monitoring,"[7] the security team traced the intruders back one leg to Internet service providers in Seattle and New York. However, the intruders use of multiple Internet paths and "phone phreaking,"[8] and legal delays in obtaining wiretap authority

stymied attempts to trace them to the source. Through innovative casework, the security team was able to glean the hackers nicknames. Human intelligence sources pinpointed the intruders, nicknamed "Datastream Cowboy" and "Kuji," to two locations in the United Kingdom. American security experts, working in conjunction with New Scotland Yard, were finally able to trace and arrest the intruders.

The aftermath of the Rome Labs intrusion revealed that while investigators knew the actions occurring after 23 May 1994, they were unsure if the intruders accessed the system previously. Additionally, investigators did not know the location or disposition of the classified and sensitive data the intruders illegally downloaded. Although not inflicting lasting damage, the USAF estimated the attack cost over $210,000 and an additional $500,000 in man hours spent on turning off systems, verifying systems integrity, installing security patches, and restoring service.[9]

This case study demonstrates the scope of the problem the DoD faces, a sample of the interconnections between the DII and NII, the vulnerability of the DII from threats originating from the NII, and the difficulty in stopping IW attacks under the current structure. The DoD's inextricable interconnection with the global network puts defense information systems at risk from attack by way of multiple avenues. Furthermore, like the Rome Labs security team, the DoD faces a complex and cumbersome structure dealing with unauthorized computer system entry. The DoD is only allowed to trace back intruders one connection. To extend the trace beyond one node requires a court order. Obtaining a court order can be a time consuming process and may be invalidated if the intruder changes phone lines the "trap and trace" court order authorized monitoring.[10] Finally, an "Aviation Week & Space Technology" article demonstrated the inability of

national intelligence organizations to cooperate with the DoD on IW attack response. Under current plans, the DoD would have to seek permission from NSA and CIA before responding offensively to attacks against the DII.[11]

Definitions

Before continuing the discussion defining three key terms, information infrastructure, information system and information warfare, aids understanding and establishes a contextual reference. Information infrastructures embody the interconnecting "tissues" linking computers. Like the bodies central nervous system, information infrastructures directly and indirectly link computers electronically to produce a network transcending geographic and national boundaries fusing military, civilian, and business environments together. Representing two, three, and even four dimensional lines of communication, information infrastructures link various electronic data processing, storage, and analysis centers via satellite, cellular, microwave and conventional land line communications systems. Arbitrarily broken into global, national, and defense information infrastructures, each segment subsumes the previous providing a seamless network designed to transfer voice, data, and video information instantaneously.[12]

While information infrastructures provide the interconnecting "tissue," information systems represent the functioning organs of the infrastructure. Generally comprising automated or manual electronic components, information systems acquire, process, store, distribute, and analyze information. Existing either discretely or as components of larger networks, information systems encompass the totality of an organization's ability to transform data into knowledge. While generally characterized as networks of computers, such as the Department of Defense Intelligence Information System (DODIIS),[13]

information systems also contain human analysis and interpretation mechanisms necessary to add intelligence to automated processes.[14]

While information infrastructure and systems definitions represent generally accepted principles, IW definitions represent a deep crevasse of different interpretations and definitions. While differing in scope, emphasis and content, IW generally embodies actions, either offensive or defensive in nature, designed to preserve free access to information at the strategic, operational, and tactical levels while denying the same to opponents. Primarily targeting information-based processes, IW seeks to destroy, corrupt or incapacitate adversary's information systems while simultaneously assuring free flow of information to friendly concerns by constructing barriers, warning indicators, and backup systems. Conceptually, an important distinction is the idea of warfare. While IW may not represent tactical contact and tangible destruction familiar to most warfare practitioners, it is nonetheless seeks to aggressively deny a sovereign entities ability to make decisions free of coercion.[15]

Proliferation of the Information Infrastructures

Proliferation of the DII within the DoD provides a good example of the prevasiveness of information infrastructures in all levels of society. Showing no sign of abating, the DII consumes all facets of DoD operations and provides US Armed Forces with reliable and secure information infrastructures necessary to develop combat power globally. Over 2.1 million computers, 10,000 local area networks, and 100 long distance networks represents part of the vast DII enabling US Armed Forces to implement US policies.[16] Whether directing forces during full scale conflict, conducting counter-

narcotics surveillance, or paying airmen around the world, the interconnectivity backbone for the DoD is the DII.

The "virtual" links created by the DII touch all aspects of operations. Applications of the networks collection, analysis, processing, and storage capabilities include research and development, operational planning, personal administration, weapons system maintenance, and procurement. Approximately 90% of the unclassified data transit computer systems link to the DII. While most classified information is encrypted, stored in isolated networks, or transmitted only on secure circuits, the bulk of the other data transiting the DII is unencrypted.[17]

"Joint Vision 2010" and Command, Control Communications and Computers For The Warrior (C4IFTW) provides evidence of the extent to which the US Armed Forces critical dependence upon the DII permeates present and future operations. "Joint Vision 2010," guides the evolution of future US Armed Forces toward attaining the goal of full spectrum dominance. It also provides common direction for services to meet the challenges and uncertainties of future warfighting environments. To achieve the goal of full spectrum dominance, "Joint Vision 2010" combines dominant maneuver, precision engagement, full-dimensional protection, and focused logistics.[18] The critical component enabling each of these four pillars of "Joint Vision 2010" to come together and operate synergistically is information superiority and technological innovation. Implementing this doctrine for future warfighting and achieving full spectrum dominance ultimately rests on the ability the US Armed Forces ability to exploit the unhindered access to information at the strategic, operational, and tactical level of warfare.[19]

"Joint Vision 2010's" conceptual framework exists in an environment where US Armed Forces information systems and infrastructure possess the ability to freely synthesize information. Without continuous access to networked data sources, the US Armed Forces face a situation where dominant maneuver, precision engagement, full-dimensional protection, and focused logistics become liabilities versus assets and where potential adversaries reach parity or even temporary advantage. Attaining dominant maneuver's near complete battle-space awareness and improved battlefield agility requires timely access to networked based information. Similarly, precision engagement requires access to intelligence, surveillance, reconnaissance and targeting information to rapidly and accurately target and retarget attack systems, decrease fratricide, and increase probability of success. Achieving full dimensional protection requires information superiority to provide real time threat information to rear area defensive systems. Finally, rapid response and logistical agility requires secure and accessible links to the DII.

While "Joint Vision 2010" provides an overall doctrinal direction, C4IFTW demonstrates the extent to which the US Armed Forces seek to transform its entire command and control system into a worldwide interconnected network. Billed as the 21st century vision for the future, C4IFTW envisions a global infrastructure of interconnected "...computer controlled telecommunications grids that transcend industry, media, government, military, and other non-government entities."[20] Seeking complete transparency between information systems, C4IFTW uses open systems architecture to provide virtual connectivity between all nodes within the US Armed Forces. Built upon a Secret Internet Protocol Router Network (SIPR Net),[21] C4IFTW builds a distributed ground, airborne and spaced-based communications grid over geographic areas of

responsibility enabling real-time and near real-time transmission and synthesis of voice, data, and imagery information.[22]

Studying C4IFTW and "Joint Vision 2010" reveals future tactical, operational, and strategic portions of the NII and DII may overlap and continue blurring lines of control. Future battlefields may witness development of a tactical internet or intranet designed to provide real time battlefield information such as position, combat status, supply status, or battle damage assessment through automated updating mechanisms. In turn, the same information transported within the tactical Internet between units will also be linked to joint command centers, headquarters, and planning cells. By monitoring the tactical Internet, operational level planners will instantly know the status of combat forces, progress of units in close combat, or stocks of critical spare parts. Through this link, commander's will be able to instantaneously observe, orient, decide, and assess the outcome of key battles and develop follow-on strategies to achieve desired end states. Finally, links between the NII and DII, utilizing SIPR Net, will connect the tactical units to strategic authorities and grant National Command Authorities the ability to monitor the status of tactical level actions and troop losses.

"Joint Vision 2010" and C4IFTW reveals the DII plays a critical role in future warfighting missions across the spectrum of conflict. Information flow pertaining to every aspect of operations will traverse a global network. Without unhindered access to the DII US Armed Forces may be unable to effectively employ forces engaged in global security operations. US Armed Forces may operate in a future environment where geographic separation becomes increasingly irrelevant, time and space relationships continue shrinking, and demand for instantaneous communications increases. However, as the

demand for global connectivity and reliance on the NII and DII increases, the opportunities to attack the US Armed Forces information-based processes also grows. Automating and connecting new processes to the DII increases the threat from intruders seeking to disrupt US military operations. While the advantages provided by linking US Armed Forces to the DII will synergistically increase combat capability, the risks that supporting infrastructures fail or are seriously compromise also increase.

Attacks on the DII and NII

Growing dependence of the US Armed Forces on the DII and NII has not escaped the attention of those wishing to subvert US military operations. Recent history illustrates that DII and NII reliance on public switch networks, commercial telecommunications providers, and commercial computer manufacturers exposes the geographic borders of the US to a host of electronic threats. While advancements in information infrastructure technology and architecture continue ameliorating time, space, and political border constraints, it also continues exposing new areas to a "Pandora's box" of new threats utilizing electronic attack.

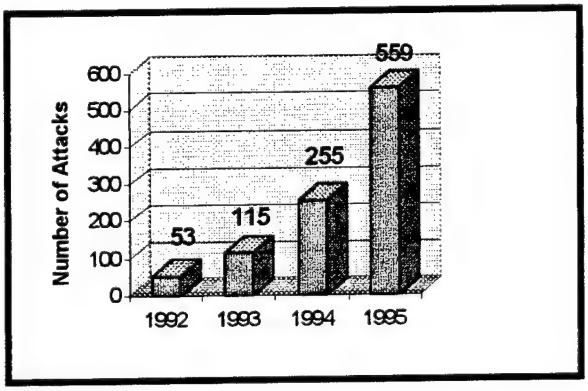


Figure 1: Number of Attacks Against DoD Computers

The increase in computer intrusions into DoD systems serves as one example of the enticing target the DII presents. Figure 1 illustrates that a Government Accounting Office (GAO) report documented the number of Defense Information Systems Agency (DISA) reported attacks against DoD

computers 1,200% between 1992 and 1995. More alarmingly, the GAO report expected the number of attacks to increase to 14,000 by the year 1999. While the number of attacks is growing at a staggering rate, the ability to detect attacks remains troublesome. DISA estimates computer users detect only one in 150 attacks. Considering these statistics, the actual number of attacks could be as high as 250,000 annually. Finally, DISA initiated security breaches revealed a 65% success rate and a 98% rate that both real and test penetrations went undetected.[23]

While the number of attacks have increased so have their severity and scope. Attackers have "stolen, modified, and destroyed data and software... They have shut down entire systems and networks, thereby denying service to users who depend on automated systems..."[24] Attacker's motives run the gamut from curious hackers seeking to break into DoD computers because of the challenge it presents to vandals attempting to cause direct damage to key computing facilities and professional thieves seeking to copy data and leave trapdoors for future access. The National Security Agency and the Department of Energy estimate that some 120 country's possess active IW programs and that most of these countries will utilize their capability to enhance security. Today's DII and NII face a global threat bent on damaging, disabling, and stealing vital information.[25]

Threats & Vulnerabilities of Information Infrastructures

Generally, the DII and NII face three classes of attackers each with differing motives. Winn Schwartau, one of the countries leading experts in computer security, characterizes perpetrators of information attack as information warriors. Information warriors range from disgruntled government corporate employees and conventional

hackers to narco-terrorists, organized criminals, mercenaries and foreign operatives. Surprisingly, Schwartau reveals many information warriors wear business suits with starched shirts and see their actions as totally legitimate.[26] As diverse as the cast of characters are so are their motives. System abuses information warriors initiate include theft of assets, acquisition and/or alteration of objective and subjective data, corruption of data in transit or in storage, and disruption of information services.[27]

This highly distributed threat utilizes hardware design limitations, software vulnerabilities, and human frailties to attack the DII and NII. Hardware vulnerabilities generally relate to shortcomings of electronic architecture and public telecommunications networks. Architectural limitations manifest themselves in the vulnerability of gateways, terminal servers, and routers to malicious and unintentional disruptive attack.[28] Routers, when remotely accessed, are easily bypassed. Gateways, when specifically targeted, are highly vulnerable to corruption or overloading,. Finally, software driven public telecommunications networks are also subject to malicious or unintentional insider disruption. Increasingly the network carrying voice, data, and video information is remotely managed by a handful of operators and technicians. As the number of specialists with the expertise to disrupt the telecommunications systems grows and the complexity of software increases so does the threat to disruption and corruption.[29]

Unlike hardware vulnerabilities, software vulnerabilities relate to use of commercial software, centralization of data storage, and unintentional or malicious destruction of key parts of code. Software vulnerabilities generally manifest themselves when disgruntled employees, intentional saboteurs, or malicious software programmers embed errors into key programs. These errors potentially create havoc in networked

environments where critical software resides in centralized data storage mechanisms.[30] An example of this type of problem is the logic bomb designed to explode upon the occurrence of a particular event or after a certain time limit.[31]

The threat facing the DII and NII are not entirely the responsibility of rogue agents, disgruntled employees, hardware and software design faults, or foreign governments. Many of the vulnerabilities of US computer systems stem from poor internal security. Human factors, such as poor password protection, physical security, and lack of vigilance by system administrators coupled with requirements for open network architecture,[32] and weaknesses in protocol-based authentication and cryptosystem security contribute to a majority of the vulnerabilities.[33]

Summary

The DII dominates the landscape of the US Armed Forces. Seemingly every facet of operations will in some way be connected to the vast network of information systems connected by way of national and global telecommunications networks. Whether it is the President watching weapons impact in real time, or pilots receiving new target information, the US Armed Forces will rely on the DII to link disparate information systems to produce synergistic increases in combat power. However, while the promise of defense interconnectivity is enormous, the potential for adversaries to disrupt US Armed Forces operations before engaging in conflict is just as great. National and global telecommunications media the DII uses to distribute information opens the electronic "barn door" to a whole host of threats seeking to disrupt information based processes. No longer will US Armed Forces have the luxury of working from within secure national

borders protected by friendly neighbors and large expanses of water. This new threat, immune to physical barriers, will attack from any number of electronic venues using a myriad of electronic techniques.

The symbiotic relationship between the NII and DII and tenuous situation previously presented yields two issues—the best to method to protect the NII which serves as the backbone for all DII operations and who should be responsible for implementing the protection. Addressing methodologies for protecting the DII and NII entails developing a protection strategy and distilling from that strategy the pool of actors with the potential to fulfill the requirements. Addressing who is best able to implement the strategy also involves identifying key tasks which must be performed to adequately protect the NII.

Chapter Two: Elements of Strategy

While many different methods are available to develop strategy, the most effective method to conceptually organize NII protection efforts is an analysis using strategic and operational level planning constructs. Identifying Centers of Gravity (COG), objectives, end states, and specified tasks ensures courses of action address key vulnerabilities, build on inherent strengths, accomplish intermediate objectives, and achieve desired ending environments. The broad nature of the NII and the vast array of information systems and electronic architectures dictates clearly defining and articulating key COG to ensure the plans remain focused on areas vital to the NII. Articulating NII COG also defines the bounds for protection strategies ensuring efficient use of resources. Carefully defined objectives and end states clarify the ending environment, establish desired outcomes of individual actions, and illustrate vital national interests that must be protected. Key task specification outlines the building blocks courses of action utilize to construct a viable protection plan. It also assures the strategy's solid foundational underpinnings. Defining, analyzing, and combining key strategic planning concepts ensures identification of critical strengths and weaknesses, clear definition of objectives and end states, and careful determination and delegation of required tasks.[34]

DII and NII Centers of Gravity

Clearly to say any strategy protecting the NII must afford complete protection is absurd. The facts that over three billion computers currently exist, predicted exponential growth in computer use until the year 2005, continued doubling of microprocessor performance every 18 months, and as many as one hundred million people accessing the

Internet by the year 2,000 militates against such as response.[35] Therefore, any protection strategy will not protect universal access, complete interconnectivity, or every critical information system.

One method to focus and constrain protection to key elements of the NII is COG analysis. Colonel John Warden in his book, The Air Campaign, defines COG as:

> ...that point where the enemy is most vulnerable and the point where an attack will have the best chance of being decisive. The term is borrowed from mechanics, indicating a point against which a level of effort ... will accomplish more than that same level of effort could accomplish if applied elsewhere. Clausewitz called it the 'hub of all power and movement.'[36]

To facilitate identifying critical COG, Warden viewed an adversary as a system containing five concentric rings. These five concentric rings include leadership, organic essentials, infrastructure, population, and fielded military forces.[37] Within each of these rings a COG or series of COG exist representing the "hub of all power for that ring." If that COG is destroyed, the entire ring ceases to function and the enemy as a system collapses. In his reductionist approach, to identify the COG for a particular ring, Warden proposed continually breaking down each ring into the same subset of rings in the original model. As each ring is continually dissected, critical nodes related to each COG will appear. These nodes represent vital areas which must be attacked or defended.[38] Applying his reductionist approach to the NII produces critical vulnerabilities to orient information protection strategies and enables strategists to focus limited resources. As an analytical tool, identifying COG defines the source of friendly and enemy strengths and weaknesses and where the strategic plans must mass effects to attain decisive victory while building defenses to prevent defeat.[39]

Utilizing Warden's model reveals that all five COG sub-categories fundamentally rely on information to function effectively. Information and advanced technologies enabling rapid information processing, serve to control various facets of the NII. Information also serves as both the ordering and control mechanisms governing complex processes. It governs the functions of individual components of the NII while simultaneously being transported through the NII to serve as input to other ordering and control mechanisms.[40] In like manner, whether viewed in a military or civilian context, information and associated advances in technology serve also transforms every aspect of the US's ability to create wealth, promote national security and stability, and project military power. In a military context, information is a vital element in applying operational art to modern combat forces. In a civilian context, information increases efficiencies and reduces factors of production. Because of the critical role it plays within today's information based society, information is the NII COG protection strategy must focus upon.[41]

Demonstrating information is the COG for the US Armed Forces involves examining the role it plays in organizing and describing fielded military forces. Information, and the ability to manipulate it, continually brings order to complex and multifaceted combat operations. The increasing complexity of operations, the inability to defeat an enemy with a single blow and the resulting emergence of operational art, requires the US Armed Forces plan and control complex distributed operations.[42] Information is central to accomplishing this task and controlling protracted military operations and campaigns. It provides feedback on past operations while directing future

operations toward mission outcomes. Without information, bringing order, control, and simplicity to complex military operations becomes exceedingly difficult.[43]

While the US Armed Forces rely on information to organize and describe itself, other trends signal the military's critical reliance upon information. Information and advanced information access mechanisms continue fueling drives toward de-massification, digitization, and automation of key combat forces and capabilities. The ability to increase combat lethality, decrease physical size, and flatten military organizations centrally depends on access to information.[44]

A similar information transformation is taking place in the civilian sector. The roots of the metamorphosis of the US to a third wave information based society lay in information utilization and advanced information technology. The ability for business and industry to efficiently utilize factors of production, streamline mass production practices, transform bureaucratic management structures, and accelerate the pace of operations all rely on information.[45] Radical transformation of national telecommunications, financial, transportation, and electrical infrastructures is also grounded in advanced information processing mechanisms. Information age technologies now control every aspect of the nations critical internal infrastructures allowing unprecedented information sharing, remote centralized control, and increased operational efficiency. Increases in human efficiency are due in large part to automation, digitization, and connection of more systems to the NII. Information and information access is quickly becoming the critical hub of power essential to future national survival.[46]

Completing NII COG analysis also requires analyzing where critical vulnerabilities to the information COG reside and where information attack can produce the greatest

effect. Further inspection reveals key systems in each COG where intentional or unintended information attack, manipulation, or destruction could severely damage critical NII capabilities and drastically effect the information COG. These key systems represent points where attackers gained a marked advantage[47] and defenders derive freedom of action.[48] Figure 2 depicts key vulnerabilities for each COG. Under leadership, decisive impact occurs when information warfare and manipulation prevents command and control networks from directing fielded military forces or internal workings of the federal

Centers of Gravity	Leadership	Organic Essentials	Infrastructure	Population	Fielded Military Forces
Critical Vulner-ability	-Command & Control Networks	-Electric Power -Gas/Oil Pipelines -Federal Inter-state Funds Xfer System	-Telecommun-ications systems -Public Switch Network -Internet -Transportation Dispatch	-Human services -Public News & Information -Disaster Res-ponse and Relief Systems	-Communications networks -Logistics & Per-sonal Databases -Transportation Management -Computer Aided weapons systems

Figure 2: Key COG and Critical Vulnerabilities for NII and DII Protection[49]

government. In the area of infrastructure and organic essentials, manipulating information contained in energy, banking, transportation, human services, and telecommunications infrastructures drastically degrades their ability to provide the framework for strong national defense, economic prosperity, and enhanced quality of life. The integration of critical infrastructures, via a national computing network, produces synergistic increases in national power and economic security the nation vitally depends upon. For fielded military forces, information warfare and manipulation directed toward communications networks, logistics and personal databases, and transportation management systems hinder the ability to deploy and employ forces. It is these critical nodes and their electronic links that represent critical vulnerabilities to NII where protection efforts must focus.[50]

COG analysis provides a subset of information systems and infrastructures focusing NII protection strategies. However, within this subset of critical COG further stratification is necessary. Any information infrastructure protection strategy must ensure a set of Minimum Essential Information Infrastructures (MEII) remains viable. This MEII represents core functions and systems assuring viability of national information based processes should wide scale outages or coordinated IW attacks occur. Conceptually, the MEII is a set of secure and segregated communications, services, and management structures necessary to perform key functions. Built around secure gateways and networks, the MEII is composed of components from Milstar, Government Emergency Telecommunications Service, Telecommunications Service Priority System, and National Telecommunications Management Structure. It functions to restore critical energy, communications, and financial sectors in times of crises and assures continuity of national executive, legislative, and military control over conventional and nuclear forces. A 1995 "Defense Science Board (DSB) Summer Study" described the MEII as a fail-safe network of minimum infrastructure and restoration capabilities independent of the public switch network and suggested action be taken to identify and prioritize minimum essential conventional force structure requirement and design and fund MEII fail-safe capabilities.[51]

In summary, the key NII COG is information, information systems that transform data into useful means, and the information that facilitates control over the NII. In this sense information is the data with meaning and purpose necessary to control complex NII sub-processes. Within the information COG, separate subsets of information related processes, critical functions, and infrastructures represent areas of critical vulnerability. The most critical functions requiring the greatest protection revolve around critical system

comprising the MEII. NII protection strategy should orient toward protecting the information COG, its critical areas of vulnerability, and associated electronic links.

Strategic Objectives and End State

Of equal importance to understanding NII COG is defining the objectives a protection strategy seeks to achieve. The essence of building a strategy to protect the NII involves defining national information objectives and strategic end states and then building a strategy designed to satisfy both. Broad strategic and operational objectives provide the vector focusing all actions, key tasks a plan must accomplish, and themes around which to build the entire plan.

The process of defining key objectives and end states normally begins by analyzing vital national information interests and objectives outlined in a national information policy. Although the US does not presently specify a national information policy, it is possible to synthesize objectives and end states from national policy themes outlined in The National Security Strategy (NSS). Serving as the cornerstone national policy document, the NSS three national goals are: "To enhance our security with effective diplomacy and with military forces that are ready to fight and win. To bolster America's economic prosperity. To promote democracy abroad."[52] Specific national objectives cascading from these national goals include stable and secure financial structures, robust military forces with the ability to react globally, sound domestic infrastructures ensuring national stability, continuous access to emergency services in cases of local of national disaster, and assured government and constitutional authority. Each of these key political, military, and economic objectives vitally depend upon reliable, secure, and available financial, electrical,

telecommunications, and transportation infrastructures. In turn, each of these core infrastructures relies on continuous information flows. Therefore, the essential objective for an information infrastructure protection strategy involves maintaining an environment of uninterrupted information flows, integrity of national networks, and safe, secure and reliable electronic linkages free from intentional or unintentional disruption and malicious attack. Strategically, objectives orient on those NII components vital to political, military, and economic interests. Operationally, the NII protection plan focuses on protecting the information infrastructures supporting key internal domestic infrastructures.[53]

Closely linked to accomplishing the objective of maintaining uninterrupted information access is the end state of information assurance facilitating the exploitation of information differentials.[54] Information assurance involves actions undertaken to guarantee availability of NII services and integrity of information contained within the NII.[55] Information differentials are synergistic effects created when superior access to accurate and timely information is combined with new and innovative applications to produce an environment where possessors overwhelmingly dominate various sectors of society. At the strategic level, the end state is characterized by an environment where information assurance is achieved and all sectors of society can exploit information differentials necessary to produce dominating combat power and economic wealth. Achieving information assurance ensures the NII remains free from the negative effects of corruption and disruption, and the information transmitted through the infrastructures is available and accurate. Information assurance also enables a "third wave" society to develop economic, political, and military power by protecting its ability to freely collect,

process, store, and disseminate information. Without information assurance full exploitation of information differentials is virtually possible to achieve.[56]

Elements of Strategy

COG analysis reveals critical vulnerabilities of the NII. Objective determination and end state analysis describes what ends an information infrastructure protection strategy must achieve. The next element in building a strategic design for protecting the NII is defining the means to implement strategy and corresponding specified tasks the strategy must accomplish. Elements of strategy and specified tasks provide the building blocks to formulate an executable course action designed to accomplish the objective. Components of strategy and corresponding specified tasks generally fall in three categories—policy, organization, and system design.

The first key element of NII protection strategy involves defining national information policies. Clearly defined information policy serves several functions. It outlines how the US will deal with actors and agents in a networked world and clearly defines goals, intentions, and vital interests of an information-based nation. It gives notice to allies and enemy's alike the vital national interest information infrastructures play in the internal domestic environment of the United States and announces policy should threats to information interests arise. A national information policy also outlines the standards an information based society will use to form its core values, international interactions, and behaviors. Internally, a national information policy serves as a forum for consensus building by quantifying the importance of information, establishing ownership criteria, clarifying information's intangible value. It delineates guidelines for federal, state, local,

and commercial entities to develop courses of action dealing with the myriad of information based issues. National information policies provide order to an arena where few rules exist and with great potential for electronic anarchy.[57]

A national information policy also addresses the legislative and military approach federal authorities will take to defend information infrastructures. Information policy guides key decisions concerning adoption of laissez faire or "seizing the initiative" approaches and determines the intrusiveness of protection strategies.[58] It also signals the role deterrence plays in an information strategy and those actions that may initiate offensive response.

For a national information policy to effectively protect the NII it must be coupled with actions taken to clarify roles and responsibilities. The sheer size and scope of the NII precludes any attempt to centrally defend all information systems. This requires any NII protection strategy address boundaries or areas of responsibility for federal, state, local, personal and commercial authorities while simultaneously building a framework for intergovernmental and non-governmental cooperation. It also requires any NII protection plan to carefully coordinate civilian and governmental efforts.

In addition to defining national policies and roles and responsibilities, information infrastructure protection strategies must also address the task of gaining, maintaining, and exploiting information superiority. Information superiority is the dominating ability to control information systems and ensure uninterrupted flow of information. It provides an environment where the ability to exploit information differentials remains intact.[59] Like air superiority, it can be local or general and does not connote full control over the entire information spectrum. Rather, it assures those under its protective electronic umbrella

freely operate without the threat from significant attack or disruption.[60] Without information superiority the ability to share information and ensure its validity decreases and responsiveness and efficiency of information based processes wanes. Additionally, a narrowly focused information dominated society relies on information superiority to ensure critical functions and infrastructures posses the ability to gather, process, analyze, and disseminate information.[61] Whether in the battles and engagements of Desert Storm or trading actions on The New York Stock Exchange, information superiority facilitates rapid observation, orientation, decision, and action.

Future systems design requirements are a final area information infrastructure protection strategy must consider. Information systems protection represents a matrix of four possible choices (see Figure 3). The vertical axis represents the degree of required access. The horizontal axis represents resource allocation options. The combination of

Security Choices	Scrimp on security	Spend on Security
Tighten Access	Users are kept out or must alter work habits	Users can get in with effort, but no hackers can.
Loosen Access	systems are vulnerable to attack	Users can get in easily but most hackers cannot.

Figure 3: Information System Protection Choices[62]

each choice represents key decisions for policy makers. For example, decisions to make system totally closed and relatively safe may make it exceedingly difficult for authorized users to use the system for legitimate purposes. Similarly, decisions to tighten access and spend liberally on security may force users to take extraordinary means to access a system. Information infrastructure protection strategy must balance the tensions between the requirement for robust security measures and the need for free and open access to electronic media.[63]

Specified Tasks

Analyzing the elements of strategy reveals five key tasks that must be sequenced and accomplished to achieve information infrastructure assurance and superiority and protect the NII. The tasks include preventing and mitigating infrastructure attacks, formulating information policy, sharing information on NII threats and best protection practices, conducting incident management or damage control, and implementing consequence management or attack assessment and restoration.

Preventing and mitigating infrastructure attack involves thorough examination of information infrastructures at the individual owner and operator level. The intent is for infrastructure users to assess vulnerabilities and weaknesses and implement protection appropriate protection practices. It involves examining critical functions and the essential information infrastructure necessary to perform these functions. Accomplishing this task requires prioritizing key information system and components, defining critical to functions, and building protective measures around these critical components.[64]

Along with assessing information infrastructure vulnerabilities, an additional task is defining national information infrastructure protection policies. Based on assessed threats, specified objectives, and environmental analysis, policy formulation signals the strategic direction the nation will take in deterring information attacks on the US. It also specifies laws, rules, regulations and Rules of Engagement (ROE) under which forces will operate within when developing NII protection strategies.[65]

The final three tasks, sharing information infrastructure threat data and protection practices, conducting incident management, and implementing consequence management, involves specifying actions taken to facilitate attack warning, attack response, and damage

control. Information sharing involves not only the traditional intelligence functions of environmental monitoring, incident detection, and reporting but also includes synthesizing information and disseminating it to individual and corporate infrastructure users. Incident management involves actions taken to deter attacks and should deterrence fail to stop attackers by either offensive or defensive measures. Finally, consequence management involves estimating the damage caused by information attacks and implementing mechanisms designed to restore minimum information infrastructures capability.[66]

Summary

Developing a course of action to protect the NII ultimately rests on combining various elements of strategy into a coherent framework that achieves strategic end states and objectives while simultaneously protecting key vulnerabilities. For the course of action to skillfully direct resources toward the aim of information assurance, it must closely examine how to jealously protect information and the information infrastructures that transport, process and store it. It must also address accomplishment of key tasks involving attack mitigation, strategic warning, attack response, and damage control.

While elements of strategy, COG analysis, and essential task identification provide the essential ingredients necessary to develop a coherent NII protection strategy, a larger question remains unanswered. Who is best aligned to take charge of combining these elements of strategy and implementing the resulting course of action? Seemingly, the ability of the DoD to protect vital national interests and ensure stability and security conducive to economic growth and prosperity points to their personal responsibility for NII protection. Safety and security of the NII, through DoD facilitation, provides an

environment where national telecommunications, financial, and other infrastructures operate free from malicious subversion and intrusion. While many parties, both civilian and governmental, are vitally concerned with ensuring the NII remains free from disruption, their interests vary significantly. With such varied interests, the DoD appears the logical choice to protect the NII.

However, to propose the DoD take on direct responsibility for domestic or civil defense of the NII raises concerns in many areas. At the heart of the issue is whether the DoD has the legal authority, economic ability, and moral imperative to actively protect a structure not purely for military use. Structural concerns involving what agency, government or civilian, are best suited to accomplish NII defense is an additional contentious issue. Finally, areas involving constitutionally mandated freedoms and the extent to which the DoD can conduct domestic internal defense add further complexity to the debate. Therefore, the debate now turns toward addressing the central issue of whether the DoD, because of its intricate connection to the NII, has a primary or supporting role in defense of the National Information Infrastructure.

Chapter Three: Paradigms and the DoD Role

Prologue: Information Age Paradigms

Addressing whether the DoD should take the lead in protecting the NII requires discussing the effect of four information age paradigms on decisions to delegate information infrastructure protection. By fundamentally altering the operational environment, each of these paradigms impacts any role the DoD may play in NII protection. They also outline environmental bounds NII protection strategy must function within and indicate qualities an organization tasked to protect the NII must posses in order to operate effectively. Finally information age paradigms serve as benchmarks to judge whether an organization currently possesses required capabilities to protect the NII or the extent to which they must adapt to meet new requirements. These four new information age paradigms involve the impact of information on traditional dimensions of conflict, the transition of power in the information age, the impact of information on decision making, and the effect of advanced information infrastructures on global relationship.

The addition of information as a new dimension of conflict is the first major paradigm shift effecting any future role the DoD plays in NII protection. Future warfare will transcend physical media of land, sea, air, and space and include the cybernetic and electronic domain of information. This shift requires nations, seeking to secure vital national interests, control the information spectrum. The addition of information as a domain of warfare also globalizes the battlefield. Past military theorists postulated the fighting front would closely link to the industrial rear. The information age serves to

continue this trend toward an expanding battlefield. In the information age, information infrastructures radically transform the area of operations by instantaneously connecting deep and rear battle areas to the physical confines of the US. The transcendence of physical barriers by the addition of the information dimension requires future combat forces operate in an environment where information attacks in the Continental US (CONUS) will immediately impact fielded military forces. Inclusion of information in to traditional dimensions of conflict may also radically transform the decision making environs of warfare by allowing National Command Authorities to globally direct tactical combat forces in real time. The overwhelming victory in Desert Storm provides one snapshot of this new reality. Operations in Desert Storm spanned the spectrum from local[67] command and control over fielded military forces, to development of global logistical re-supply lines, and utilization CONUS based missile warning assets to track theater ballistic missile launches.[68] Future combat will require a nations military forces to create an environment where information superiority is sought and maintained globally.[69]

The use of information and IW also alters the pace of operations, opens the door to a new spectrum non-national adversaries and actors, and places critical national capabilities at risk. Information and IW dramatically changes the face of future warfare by allowing defenders and intruders to think, act, and react in near real time. Information and IW also provides adversaries and allies the ability to strike directly at a nation's vital centers once protected by extensive physical barriers.[70] The advent of advanced IW techniques, such as E-mail bombs, logic bombs, pinging, computer hijacking, and viruses, allows intruders, such as terrorist groups, business cartels, and criminal organizations, to circumvent traditional defenses and strike with impunity across geographic and temporal

boundaries.[71] Information and information warfare complements traditional domains of warfare and is a new dimension of warfare where governments, militaries, and corporations seek to achieve political and economic objectives.

A second information age paradigm deals with the source of power in an information based society and the effect information technologies will have on the decentralization of power. Power will rest in the hands of those with the ability to gather and use information faster than adversaries. Information and information systems produce distinct advantages and vast power in the hands of those who can process, distribute, analyze, and store information faster than opponents. In this new reality, power will rest with those nations, organizations, and commercial entities who can quickly manipulate information and develop the ability to observe, orient, decide and act faster than adversaries.[72] Furthermore, as a result of new information technology, power will become highly decentralized as traditional organizational hierarchies continue breakdown. Previously, power in rigid vertically centered organizations emanated from the apex of the organization downward. However, as organizations transition toward horizontal hierarchies, power will become diluted from the upper echelons and will rapidly distribute itself throughout the organization.[73] A report by the National Defense Panel sums up where power will reside. "The entity that has greater access to, and can more readily apply, meaningful information will have the advantage in both diplomacy and defense."[74]

Balanced against this new information age paradigm is the old paradigm that information and information technology will not produce increased certainty in decision making. Where human will and emotion dominate, independent will exists, and the hunger for information feeds upon itself, uncertainty in decision making will dominate the

environment with or without advanced information age technologies.[75] Furthermore, the proliferation of advanced information distribution technologies and the rise of 24 hour global media coverage may increase decision making uncertainty by forcing leaders to rapidly react to changing events without the benefit of clearly thinking through outcomes.

Changes to the physical security environment of the US is the fourth information age paradigm. No longer is the US protected by broad oceans and friendly neighbors. Porous electronic borders and diverse information age threats present global security challenges to US internal stability. Electronic linkages across global information infrastructures continue eroding traditional physical sanctuaries. Reliance on information age technologies also makes the US vulnerable to attacks across both physical and electronic media. Unlike cold war paradigms, the erosion of traditional physical defenses exposes the US to new trans-national threats such as hackers, drug cartels, economic terrorists, and hate groups. While nation-states will continue dominating international systems, increasingly power will gravitate toward multinational corporations, and other legitimate and illegitimate transnational actors. Formation of new alliances reflecting electronic interconnection and interdependence will arise as technology continues to alter geopolitical, cultural, and social landscapes. The trend toward globalization will increase the number of actors seeking to impose their political and economic agendas on the US and increase the complexity of global political relationships.[76]

Can the DoD Handle the Job Alone?

Given contextual changes to the US security environment, the discussion now turns toward answering whether the DoD should take control over NII protection. The

issue revolves around whether the DoD should protect the NII for national security reasons when the majority of the ownership resides with private carriers and citizens.[77] Based upon aforementioned national security objectives and strategic end states, policy makers and military proponents argue the DoD should play the lead role in protecting the NII to assure the US maintain information superiority. However, looking beyond constitutional mandates, national security concerns, demonstrated planning expertise, and shortcomings of the commercial sector, protecting the NII is a broad and complex problem extending beyond the capability of the DoD. Demonstrating the fallacious nature of arguments for the DoD playing the central role in NII protection requires reviewing various reasons pundits put forth supporting the DoD's central claim upon NII protection and then demonstrating how these arguments inadequately address larger issues involving impartiality, privacy, free speech, and separation of powers.

Various reasons point toward nominating the DoD as the dominant force in NII protection strategy. The first argument for DoD as lead agent in NII protection encompasses the traditional role it plays in protecting national interests. The more dependent a nation becomes on the integrity of information infrastructures, the more they become vital national interests. Any threats to the NII, as vital national interests, requires implementing some form of protection to ensure they remain protected from external intrusion. As the traditional agency charged with protecting the US "against all enemies, both foreign and domestic,"[78] much of the responsibility to protect vital US national interests falls under the purview of the DoD. Therefore, because the national security, domestic stability, and national economic, cultural, and social well being is at stake, some argue the DoD should serve as the central authority countering threats to the NII.[79]

Policy makers also argue split allegiances of the commercial sector disqualifies them as candidates to protect the NII. Commercial entities argue against government protection of the NII by stating they could implement the same protection more efficiently. However, conflicts will certainly arise in organizations chartered to maximize shareholder profit and also directly tasked with national security concerns. The rationale against commercial defense of the NII does not involve patriotism. Rather, the issue revolves around whether commercial organizations have the resources, technical competence, and incentives to implement robust NII protection strategies and whether the nation wishes to entrust matters of national security to commercial organizations. The reaction of commercial organizations to the ethical conundrum of balancing the corporate bottom line against national security interests is ground best left uncultivated.

In addition to national security arguments, other pragmatic reasons point toward the DoD playing the lead role in NII protection. Potential undermining of the NII could have devastating impacts on conventional warfare capabilities. In an era of downsizing and force projection, any attack on the NII could directly undermine the US ability to project power. Careful consideration should also be given to the vast planning expertise and resources of the US Armed Forces. The US Armed Forces and DoD's keen understanding of planning operations in support of national security objectives provides valuable experience in dealing with the complex issues involved in NII protection. Coupled with operational experience, the DoD also possesses powerful deliberate and crises action planning systems necessary to implement future NII protection plans.

Finally, while less bloody, information attack is still a form of war meant to impose political will of the aggressor. Whether waged on a battlefield or computer terminal, the

intent of information war is manipulation of the sovereign action of another nation. The aim is to deny the attacked entity the right to make choices and decisions free from coercion. In this light, IW's sole purpose is to conduct warfare designed to steal, damage or destroy information and thus is the domain of the US Armed Forces and DoD.[80]

On the surface, each of these arguments for the DoD playing the lead role in NII protection seem justified in light of national security concerns. However, while seductive in their logic, each of these points fail to address deeper contextual issues. Advocating DoD play the lead role in NII protection ignores major policy issues related to deeply cherished and constitutionally mandated free speech and privacy rights guaranteed to all citizens. They also fail to address whether the DoD has the capacity to adapt present conventional warfare capabilities to meet the challenges of an information age problem and whether the DoD can vault past internal organizational differences and squabbles over doctrine and funding to come together to effectively protect the NII. Equally lacking from the debate is whether the DoD has the ability to objectively balance economic, political, and social interests directly competing with national security interests. Finally, each of the above the rationale for DoD ascendancy in NII protection fail to discuss the reaction of a pluralistic society to concentration of power in one arm of government. It for these an many more reasons that the DoD should not play the central role in protecting the NII.

To argue the DoD should play the lead role in NII protection because of compelling national security interests, demonstrated expertise in warfighting, vast resources and planning experience, or the shortcomings of the commercial sector ignores the depth and breadth of the task. Furthermore, it also ignores political, legal, and moral implications of such decisions. The vast nature and complexity of the NII outstrips any

one agencies capabilities. Furthermore, balancing the need to protect a complex interconnected information infrastructure and with needs of a pluralistic society requires careful consideration of all issues involved; a task which may fall well outside of the legal and constitutional mandates of the DoD.

Maintaining the DoD should be the lead agent in protecting the NII assumes the US Armed Forces have both the understanding of the underlying complexity of the problem and the ability to manage the solution. However, it is unclear whether a military built to fight in the physical domain has the capability to counter threats in electronic domain. The US Armed Forces represent a force with no equal in conventional capability. But, as overwhelmingly powerful as conventional forces are in engaging in modern warfare, the applicability of current doctrine, equipment, and training and the ability to rapidly adapt to new threats and security challenges facing the NII remains a significant question mark.[81] Overall conservatism of the military establishment, immense institutional inertia, and myopic views toward changing environments may also signal that the DoD does not possess the ability to meet the security needs of a complex adaptive environment.

Equally uncertain are broad legal issues involved with the DoD utilizing offensive means to intrude on the privacy of US citizens. Protecting the NII entails utilizing a combination of offensive and defensive means to secure the system both globally and domestically. It remains unclear if authority to protect the NII also includes authority to launch domestic IW operations. Equally murky are ramifications of domestic operations in light of Posse Comitatus barriers in place to prevent military intrusion into civil affairs.

The DoD's ability to honestly consider the interests of varied stakeholders is further rationale against their role as prime protector of the NII. The NII represents a

complex environment filled with many actors utilizing a single medium to perform key functions. While the common thread linking diverse groups is the requirement to use the NII, their purposes differ vastly. In this networked world, stakeholder interests clash as differing groups see the NII from independent world views. Protectors of the NII must be able to balance constitutionally mandated personal protection, national security concerns, stakeholder interest, and American notions of individual liberty. This environment produces situations where it may be difficult for the DoD to serve as the honest broker and balance military necessity with diverse economic, academic and political interests.[82]

While the ability of the DoD to respect various stakeholder interests remains questionable, an additional concern is the DoD's ability to deal with an environment where national security concerns blend with economic and social concerns. NII stakeholder interests do not singularly encompass political, military, economic or social environments but rather represent a blending of all three. Whereas national security could take center stage in a world not as electronically interconnected, today national security concerns must compete with economic, social, and political concerns traversing national information pathways. In this brave new "wired" world, civil libertarians and academics free speech interests, entrepreneurs market concerns, and national security interests begin to merge and create a melting pot of interests and ideas. "In an age ... when production is measured more in terms of intangible knowledge than tangible goods, and when the value of knowledge applies equally in both civil and military sectors, the distinction between the two realms will blur even more."[83] The competition from other national interests may signal the end of authority and action based solely on national security.

While impartiality and complexity may militate against the DoD as lead agent for NII protection, the values of a pluralistic society also rebel against such efforts. A pluralistic society will not allow gravitation of immense power in the hands of the DoD. The inherent mistrust of such vast power in hands of the military and the potential for its misuse in the heart of America's violates the nations constitutional ideals of shared power. Furthermore, it moves dangerously close to a system where the military moves into the arena of policy determination. Some argue the military, through it's strategic planning processes, has always defined and elaborated policy.[84] However, to move the DoD into the position of determining what is best for nation based on national security concerns runs the risk of turning a force meant to protect national interests in to a force where national security becomes the prime concern. Military control over NII protection runs counter to the concepts of shared authority and may jeopardize foundational freedoms.[85]

Interservice rivalry also signals existing structures within the DoD may not be best suited to handle NII protection. Whether it is intense debate over weapons programs and budget allocations or disagreements over definitions and doctrine, the internal environment within the DoD may not be best suited to fulfill the role. One example supporting this argument is the battle between the intelligence community and the DoD over the use of offensive IW. From those close to the situation, a debate rages between the national intelligence agencies[86] and the DoD on use of offensive and defensive IW. National intelligence agencies aim to roam freely and listen to targeted networks. The military community aims to listen then attack. Cross purposes, compartmentalization of information, and bureaucratic roadblocks do not bode well for an organization that must come together and protect a system vital to all residing within US borders.[87]

Finally, myopic approaches to IW strategies also signals the DoD may not be best suited to protect the NII. Currently each service's IW development initiatives rests in the wartime subsets of IW. The focus of all services have thus far concentrated on achieving information dominance for fielded military forces in major wartime environments. However, comprehensive development of wartime IW capabilities falls far short of the requirements for protecting the NII as a whole. While developing these capabilities are important they represent only a small part of the overall requirements necessary to comprehensively protect the NII.[88]

Summary

While traditional national security concerns, extensive experience in deliberate planning, shortcomings of commercial organizations and the characteristics of war may indicate the DoD serve as lead agent in protecting the NII, many compelling reasons exist militating against such actions. Complex issues involving personal privacy, protection of individual liberties, and constitutionally mandated separation of power dictate against centralized DoD control of the NII. The need to balance various stakeholder interests and the concerns of a pluralistic society also argue against the DoD protecting the NII. Finally, shortcomings in training, doctrine, and equipment, and interservice rivalries also signal the DoD should not serve as central defensive authority over the NII.

While many reasons argue against the DoD centrally protecting the NII, none is more compelling than the physical nature the medium. The NII represents a highly decentralized network of users and information systems and efforts directed toward centrally controlling NII protection efforts runs counter to the problem at hand. The NII

is threatened by agents whose speed and complexity continually shrinks dimensions of time and space while simultaneously accelerating the pace of operations.[89] The US no longer possesses the luxury of time to orchestrate war plans countering electronic attacks occurring within minutes from threats utilizing a dozen different means.[90] Countering a distributed threat, attacking through multiple means, requires a system executing operations at the point of impact. The increase in velocity of IW and the breadth of the electronic threats prevents a handful of commanders centrally controlling NII operations. An environment, where threats could attack numerous sites simultaneously, requires NII protection plans be based on individual responsibility and cooperative action.

The spontaneity and chaos of the information environment coupled with the necessity to possess intelligence at the point of impact also militates against centralized control. The IW environment, its ability to instantaneously produce new threats, and their ability to attack from hundreds of different sources, presents the intelligence community with a challenge to cope with a real time threat. The ability for individuals to react "just in time" may be critical to stemming the onslaught of an all out IW attack. In this amorphous and chaotic environment, intelligence must be agile and decentralized to cope with the myriad of potential threats.[91]

After establishing the DoD should play a role but not the central role in protecting the NII, the discussion now turns to analyzing where to employ its capabilities. The discussion involves addressing the performance of five key tasks to protect the NII, how these tasks should be accomplished, and by whom they should accomplished.

Chapter Four: A Strategy for Protecting the NII

If the DoD cannot singularly take responsibility for protecting the NII then the question becomes what role should they play? One method to clarify the DoD's role in NII protection is analyzing which organizations or individuals are responsible for accomplishing each of the five key tasks involved in NII protection and which key tasks individually or organizationally remain the responsibility of the DoD. As a review, the five key tasks involved in NII protection are policy formulation, information sharing, attack prevention and mitigation, incident management, and consequence management. This approach ensures accomplishment of critical tasks by those best qualified. It also guarantees clear delineation of individuals or organizations with primary responsibility and in the parlance of the military's command relationships, allows clear definition of supported and supporting organizational relationships. Finally, task analysis provides strategists a method to dissect NII protection through the lens of new information age paradigms, crucial information COG, and critical NII vulnerabilities. Assigning responsibility for key tasks, on the basis of COG, critical vulnerability, and information age paradigm analysis, ensures NII protection strategy addresses critical readiness and capabilities issues and the DoD's role is clearly defined and properly bounded.

Prevention and Mitigation, an Individual Responsibility

Foundationally, developing an effective NII protection strategy must first address the best method to protect a highly distributed network by assigning responsibility for attack prevention and mitigation. An effective NII protection strategy should stress attack prevention and mitigation is an individual or organizational responsibility. Emphasizing

individual and organizational responsibility involves holding each individual, organization, company, or government agency connecting to the NII accountable for protection of information systems under their direct control. The decentralized nature of the NII and the ability for intruders roam freely and attack any system connected to the NII mandates personal responsibility for attack prevention and mitigation. The fact that most of the NII falls under individual control also warrants accentuating individual responsibility. Finally, scarcity of protection resources coupled with the vast nature of the NII requires prioritization of vital national information systems and mandates allocating resource and protection priority to those systems critical to NII operation.

Any protection strategy should also emphasize personal responsibility for attack prevention and mitigation because protection of those information systems and infrastructures logically remains the responsibility of individuals. Individuals or organizations should also shoulder the burden of attack prevention and mitigation because they bear the brunt of costs associated with failure or lack of service and they possess the best capability to protect their systems. However, this responsibility should be elevated beyond local control when the information systems or infrastructures failure can have wide ranging consequences. If the owner of an information system or local infrastructure bears the totality in cost and inconvenience of failure, then its protection should fall within their purview. In this instance, the individual not only bears the responsibility but also has the financial incentive to do so. Additionally, many information systems owners employ administrative staff to handle such situations and require little outside help in dealing with recovery and repair operations. Finally, an organizations individual familiarity with internal organizational information requirements enables individuals and organizations to

tailor attack protection and mitigation practices versus having to implement protection practices built for a generic organizations.[92]

Stressing personal responsibility for attack prevention and mitigation also involves performing key tasks which facilitate a paradigm shift in minds of individuals an organizations. An effective NII protection strategy must institutionalize information infrastructure protection practices by requiring information infrastructure owners and operators conduct detailed risk analysis and vulnerability assessment. Education initiatives should also be undertaken warning users on the consequences of poor system security. NII protection strategy should also provide the required tools to individual users by developing financially feasible protection mechanisms and procuring backup systems for critical internal information systems.[93] Stressing personal information infrastructure security also entails building forums for information systems owners and operators to share information on infrastructure attacks and best protection practices. Attacks against NII components cannot be written off as a cost of doing business. Fear of government intervention, damage to reputations, or weakening competitive positions, while valid concerns, also cannot prevent owners and operators from sharing information on NII attacks. Countering infrastructure attacks through prevention and mitigation requires sharing ideas, actions, and information across all sectors of society.[94]

Complimenting individual responsibility for NII attack prevention and mitigation is development of commercial technology with the ability to operate in hostile environments. Many current software and hardware engineers, born in a environment stressing open access over system security, continue producing systems highly vulnerable to intrusion and interruption.[95] Present security efforts attempt to build perimeter defenses

without addressing the ability for systems to work in hostile environments.[96] The resulting landscape of information systems and architectures represents a virtual neighborhood where unlocking the door to one house opens the door to the entire community. Systems designers must build future systems adhering to certain standards of "due diligence" and increase the ability of systems to operate in high threat environments.[97] Additionally, they must place emphasis on designing fault tolerant software and hardware with the ability to operate in less than pristine conditions. While there must be a balance between systems security and open access, in an era of information warfare, systems design must begin to skew the balance toward security.[98]

Policy Formulation, A Governmental Responsibility

Along with emphasizing personal responsibility for attack mitigation and prevention, governmental efforts must strive to simplify and clarify information policies, legalities, roles and priorities. The national information infrastructure protection policies, laws, regulations and statutes represent a sea of complexity. Examining three critical functions reveals the murkiness of the current legal waters. In the area of privacy and access to government information 12 different laws attempt to govern such diverse areas wire and oral communication, cellular phones, cordless phones, E-mail, and electronic funds transfer. Seven laws and fourteen different agencies also comprise the universe of federal organizations attempting to protect federal information systems. Each state has separate laws and regulations prohibiting different forms of unauthorized computer access. Finally, no differentiation between actions constituting criminal acts versus acts of war exists in the current national or international legal environment.[99] Consequently, the legal

and political environment lack clear definition pertaining to the DoD's Title 10 responsibilities related to NII protection and responsibilities for answering attacks against the NII.[100]

Many of the same complexities found in the legal and regulatory environment also plague the organizational environment.[101] For example, in the area of federal information systems security, 14 different agencies and departments are responsible for protecting classified and unclassified but sensitive information. Although more clearly defined, roles and responsibilities for infrastructure availability and reliability are also spread among 11 different organizations. Likewise, the responsibility for ensuring privacy and citizen access to governmental information, an area critical to implementing NII protection, involves ten different organizations under leadership of the Department of Justice and the Office of Management and Budget. Noticeably absent from this list of organizations contributing to the debate over privacy and citizen access to government information is the DoD.[102]

Simplifying the legal, regulatory, and policy environment requires NII protection plans organize an interagency working group designed to cut through various levels of bureaucracy, legislation, and organizational interests to clarify laws, regulations, roles, and missions. Similar to the Joint Security Commission (JSC) chartered in 1993 by the Secretary of Defense and Director of Central Intelligence, this working group would examine how to revamp the legal, regulatory, and policy environments to ensure protection of key information, information systems and infrastructures The working group would seek recommendations ensuring "...flexible policies match threats; consistent and cost effective policies; fair and equitable treatment of all Americans; and affordable security."[103]

Along with simplifying the legal, regulatory and policy surroundings, strategy must also distinctly and clearly define ROE governing the US Armed Forces and other national governmental agencies utilization of offensive measures to protect the NII. Guaranteeing free and open access to the NII does not imply the DoD freely employ force without restraint. The potential for collateral damage and unintended consequences of actions taken in cyberspace dictate regulating actions. Actions taken during times of crises could also produce other unintended consequences in an interconnected world such as the dilemma of whether the US could target hostile forces utilizing the GII located in neutral countries. Policy makers must ensure any force used to protect the NII, whether utilized in retaliation or in pre-emptive fashion, be proportional in intensity, magnitude, and duration to the situation. They must also ensure use of force adheres to internationally accepted laws, treaties, and practices. [104]

To be effective, NII protection strategy must delineate legal, political, and moral boundaries. Certain synergistic strength emanates from the ability to freely allow leaders at all levels to exercise judgment, initiative, and expertise to execute NII protection techniques achieving national objectives. This synergistic strength can only be developed if laws, regulations, roles, missions, and ROE are clearly defined and coherently organized.

Information Sharing, A National Intelligence Responsibility

Thus far NII protection strategy has addressed who should accomplish policy formulation and attack prevention and mitigation. What is left is to outline the structure and responsibilities for performing the three remaining functions—information sharing, incident management, and consequence management.

Information sharing, which generally equates to traditional intelligence functions, involves surveying the threat environment, analyzing threats, predicting future adversary courses of action, and recommending methods to counter threats. Within the traditional framework of national intelligence, the responsibility for information sharing should fall under the direct purview of the combined national intelligence agencies[105] with supporting assistance from military intelligence and the public sector. The combined national intelligence communities provide the ideal framework upon which to build a comprehensive information sharing and intelligence network. In an age of rapidly emerging threats, national intelligence communities provide the capability to form a central repository for information gathering and analysis necessary to review intrusions, crimes, and vulnerabilities. Based upon their experience, intellectual expertise, and physical resources, national intelligence communities provide the best resource around which to build a central node for correlating information infrastructure threats.[106]

While the DoD and US Armed Forces possess similar capabilities and require comprehensive NII intelligence as well, they represent a small portion of the demand pool for information on infrastructures threats. Many diverse groups require different infrastructure threat information. Government agencies require information to develop laws and regulations. Private organizations demand information to implement protection mechanisms. Industry and academic institutions need information to develop new protection techniques and procedures. Tasking the national intelligence community to fulfill this need for information ensures all diverse user groups have timely access to necessary information.[107]

Taking on responsibility for information sharing requires major shifts in current national intelligence agencies paradigms. New information age paradigms, which place a premium on comprehensive information sharing, require national intelligence agencies both gather information and facilitating dialog between user organizations. Information critical to the defense of the NII must be available to those directly threatened. National intelligence agencies can not prevent vital information pertaining to critical vulnerabilities and threats from reaching the hands of those who need it most. In their role as the national repository for information infrastructure intelligence, national intelligence agencies must gather information on current threats, system vulnerabilities, and ongoing attacks and make it readily available to all users. Collection efforts must also keep pace with changing environments by gathering data from both traditional information sources and new open information sources such as the Internet. Finally, national intelligence agencies must serve as a repository for best protection practices. They must alert users to potential threats and provide proven techniques to counter vulnerabilities[108]

New information age paradigms signal these agencies must also shift away from cold war practices providing services in a new and different way. Serving as repositories of information, where users at all levels access information to combat a distributed threat, requires breaking old paradigms of secrecy and compartmentalization. The necessity to maintain security around critical information will remain in the future. However, NII threats will not allow national intelligence agencies to hide behind security classifications.[109] An intelligence community optimized for keeping secrets can not hope to function effectively in an era where the policy must be to inform. Information age paradigms require a new information sharing model where the national intelligence

community resembles a virtual intelligence network versus a information storage archive. The system must transition to an expanded partnership between national intelligence agencies, government, and individual owners facilitating information sharing about threats, best practices, and critical vulnerabilities. In this new virtual intelligence community, all players in the NII are mobilized to provide threat data, vulnerabilities, and best practices. Ordinary citizens acting as front line sensors enable national intelligence communities to collect real time threat information. Data collected in this new virtual intelligence community is processed in a decentralized analysis framework. The ability to analyze a plethora of threat information and maintain required expertise outstrips the ability of one body to accomplish such a task. It requires a decentralized team of experts from academia, business, media, and the military with the ability to link together, analyze threats, and gain comprehensive understanding of emerging security challenges.[110]

Incident Management and Consequence Management

The final two functions, incident management and consequence management involve responding to attacks, formulating the appropriate response, and restoring key services. Incident and consequence management require the coordination offensive and defensive actions across the spectrum of the NII and direct action in response to real or perceived threats. It also involves building an environment where all parties come together to share information and discuss techniques to protect the entire information infrastructure. It is within this framework that the DoD's two direct roles in NII protection emerge. First, the DoD should be directly responsible for facilitating discussion and developing consensus pertaining to comprehensive implementation of national incident

and consequence management plans. Second, the DoD should play a direct role in protection and restoration of the MEII.

The totality of NII incident and consequence management falls outside the realm of reasonable responsibility for DoD. A diffuse threat, decentralized medium, and diverse user pool dictate against the DoD dictating comprehensive consequence and incident management practices.[111] Other agencies, such as the Federal Emergency Management Agency, also provide valuable expertise needed to implement incident and management protections. Martin Libicki, a noted author on IW affairs points out the shortcomings of a single DoD commander for incident and consequence management.

> The very concept of a single government commander for information defense is tenuous. Any attempt to 'war-room' an information crises will find the commander armed with buttons that attach to absolutely nothing... In terms of policy, each sector is [information] sector is different, not only in terms of its vulnerabilities, and what an attack might do, but more importantly, in the range of policies that can be used to improve its security.[112]

What Libicki points toward is a requirement for lead agent to implement high-level coordination, information sharing, and forums to bring stakeholders together to discuss ways to implement comprehensive incident and consequence management practices.

Selecting a lead agent to implement forums discussing national incident and consequence management plans requires examining who has the preponderance of interests and where the nation as a whole will be effected most should the NII suffer attack. Upon this basis, the DoD should serve as the lead agent in facilitating discussion on implementation of national incident and consequence management plans "...because our national defense depends upon it and because ability to bring combat power to bear in support of national objectives relies on its ability to deploy and sustain American

forces."[113] Significant national security interests and existing telecommunications and information sector relationships dictate the DoD significantly impact incident and consequence management decisions.[114] It is in this light that the DoD should play the lead role in facilitating discussion and building consensus on how best to implement comprehensive incident and consequence management.[115]

The second role the DoD should play is direct protection of the MEII. While facilitation and consensus remain the overarching goal in devising key strategies to implement incident and consequence management, the DoD should be given the direct responsibility to implement actions necessary to protect the MEII. Derived from precedents set in nuclear deterrence era policies, the DoD should be assigned direct responsibility to protect key systems and capabilities maintaining the integrity of the US. In the cold war era, Executive Orders 12656, 12919, 12148, and 12472[116] gave particular agencies the responsibility to assure the continuity of the government and protection of vital national services in case of nuclear war. Extending this precedent to the information age, the DoD should also serve in the same capacity by protecting the integrity of key components of the NII and restoring key systems in event of attack.[117] In this instance rather than key services, DoD responsibilities lies in protecting the MEII and its ability to maintain a viable government, social services, and national defensive capabilities.

Key to defining DoD's role in protecting and restoring the MEII is defining the circumstances the US Armed Forces would exercise their authority. Any incident and consequence management strategy protecting the MEII can not nor should not protect those areas under the direct purview of individuals. Rather, a laissez faire approach to "trivial" security problems should be taken in the protection scheme.[118] An employable

incident and consequence management strategy also can not directly utilize centralized resources to protect against all forms of attack. The sheer proliferation of minor attacks, against which currently there are sound defensive mechanisms, prevents such an approach. Furthermore, pinpricks or slowly escalating attacks engender an inoculating response. Information systems and infrastructures containing protective measures possess the ability to self organize and adapt to new forms of intrusion.[119]

Sound incident and consequence management strategies should focus on critical information systems where coordinated, simultaneous, and concentrated attacks could produce devastating effects to a wide spectrum of military and civilian applications. To be effective, an attack strategy would have to employ blitzkrieg like tactics and take advantage of cascading effects of maliciously introduced failures.[120] Incident and consequence management strategies must concentrate on adversaries who will employ offensive tools to physically or electronically destroy vital electronic components and corrupt critical hardware and software in an effort to compromise or disable NII functions. Incident and consequence management strategies should also focus on areas where information conveyed in various media can be easily manipulated. It is under these circumstances, where a clear and present danger to MEII exists, that the DoD should intervene to protect and restore information infrastructures.

Summary

Comprehensively protecting the NII involves dividing responsibility for accomplishing five key task. The cornerstone of any NII protection strategy is personal , private, and organizational responsibility for attack mitigation and prevention. Securing a

vast distributed system of information networks can only be assured if those at the point of impact take personal responsibility for their security. While prevention and mitigation fall under direct control of individuals, policy formulation and national guidance pertaining to information infrastructure protection is the direct responsibility of the central government. The ability to bring order out of the current complex and chaotic information policy environment can only come with direct government leadership. To clarify and simplify the policy environment requires a comprehensive policy review aimed at defining key information policies, eliminating conflicting statutes, and reducing unnecessary levels of bureaucracy.

Emphasizing personal responsibility and defining a national information policy does not fully answer the difficult question of what role the DoD should play in NII protection. It is in the light of the last three functions, information sharing, incident management, and consequence management where the DoD's true functions lie. In the information sharing arena, the DoD serves as a supporting agent to national intelligence agencies. The DoD, along with many other stakeholders, provide information to the national intelligence network to build a virtual intelligence community. Directly, the DoD serves as the lead agent in building plans implementing national incident and consequence management actions involving the NII. The DoD's other primary role lies in protecting and restoring those critical MEII capabilities necessary for national survival when threatened from all out attack. It is in this light that the DoD's role is narrowly focused to protect only those portions of the NII which serve as the nations information COG.

Conclusion

Determining the proper role the DoD should play in protection of the NII involves developing a specific strategy. This iterative process of strategy development involves performing three sequential steps. It begins by analyzing the problem of NII protection to determine vital COG and critical vulnerabilities, strategic end states and objectives, and key tasks related to strategic end states and objectives. The process next outlines information age paradigms effecting strategy development to ensure protection actions remain focused and account for environmental changes in the domain of conflict. Finally, based on the previous steps, NII protection strategy development assigns responsibility for five tasks based on which organizations can adapt to information age paradigms and best protect vital COG and critical vulnerabilities. It is during task assignment that the DoD's two main roles become apparent. The primary roles the DoD plays involves two aspects of incident and consequence management. First, the DoD should be primarily responsible for protecting core systems of the NII known as the MEII. Second, the DoD should serve as lead agent in convening and facilitating national forums designed to gain consensus on comprehensive national incident and consequence management programs.

While assigning the DoD specific tasks to fulfill in an NII protection strategy ensures their completion it does not address how these tasks will be organized into a coherent course of action nor does not address macro level policies and organizational requirements. Effectively organizing each of the five key tasks into a coherent course of action requires sequencing actions, task organizing forces, prioritizing objectives, and fulfilling desired end states. One method to ensure each of these areas are completely

addressed is to utilize the campaign planning process. Campaign planning provides a method to organize specific elements of strategy to uniquely fulfill the desired end state. Joint Pub 3-0, Doctrine for Joint Operations, defines a campaign plan as "... a series of related major operations that arrange tactical, operational and strategic actions to accomplish strategic and operational objectives."[121] Building a campaign plan to protect the NII entails describing key phases and prioritized events, command relationships, and sequenced and synchronized actions designed to achieve the desired end state.

Key to building a comprehensive campaign plan which protects the NII is specification of national organizational structures. Currently many organizations, such as the Director of Central Intelligence, the Office of Management and Budget, Department of Commerce, Department of Justice, and DoD play a role in shaping NII protection policy.[122] However, there is not a single national entity within the government coordinating key actions pertaining to NII protection. The NII's interdisciplinary nature requires the President designate a single national entity to deal with NII protection. This national entity, possibly chaired by the Vice President and composed of permanent representatives from cabinet level departments, key economic sectors, and owners and operators of key infrastructures, would serve several functions. Collectively, it would be responsible for drafting and implementing a national information policy. It would also serve as the primary agency providing staff supervision for all NII related issues. In it's planning capacity, this national entity would be responsible for defining the nations MEII, developing grand strategies to coordinate NII protection activities, and developing in-depth campaign plans to coordinate actions of various protection agencies.[123]

Implementation of new organizational constructs within the federal government may radically alter future intergovernmental relationships and policies. Fulfilling its responsibilities in the NII protection may require the DoD to also undergo fundamental structural changes and radical alteration of internal operating procedures. As NII protection plans mature, military planners within the DoD may discover present structures unsuitable to accomplish new responsibilities. Along with organizational changes, tactical employment of NII protection plans may also cause revisions to existing military information policies. The emergence of new offensive techniques may force the DoD to alter existing policies to ensure automated attack response systems, electronic precision attack systems, and isolation routines are effectively coordinated within a larger protection strategy.[124]

A final area which significantly effects development of NII protection plans is the utilization of deterrence and defense as an overarching strategic approach. Currently, many plans to protect portions of the NII significantly rely on deterrence and defensive measures to prevent intrusion. Threats of criminal prosecution lie in wait for intruders bent on attacking the NII. At its root the major theme underlying this strategy of deterrence is the threat that perpetrators will be punished should they infiltrate and corrupt information systems. Some NII protection experts, arguing from cold war paradigms, believe deterrence should be the cornerstone of any future national information policy.[125]

While seductive in its logic, deterrence as a primary strategy to protect the NII suffers many shortcomings. The first shortcoming involves deterrence's underlying concept of retaliation. Within a strategy of NII deterrence, the US would reserve the right to retaliate against any attacker directly compromising information infrastructures with

punishment in kind. However, to argue the US requires a deterrence policy declaring it will retaliate against those attacking the NII seems absurd. In the course of international relations, the US has already established a firm policy in this area. Recent examples of these actions include the raid on Libya in 1986 in response to Libyan backed terrorism and cruise missile attacks on Iraq for plotting to assassinate former President George Bush. Furthermore, the concept of retaliation in kind indicates any attack against the US NII would engender a similar attack against the aggressor. However, if the attacker does not rely as heavily on information infrastructures, it seems highly doubtful any US sponsored attack on the aggressors NII would have much affect. In this instance, the US attack would require an asymmetric response with conventional military action. However, it remains unclear whether this course of action would be useful in an environment where incidents are difficult to trace to intruders.[126] The utility of such a course of action is also questionable when specifying the amount of asymmetric force required to retaliate against an information based attack.[127]

Deterrence strategies reliance on defense is also an additional limitation. Many problems are associated with over reliance on defensive measures. The problems with purely relying on defense were illustrated by the Prussian military theorist Carl Von Clausewitz. Clausewitz argued that while defense was the stronger form of warfare, attack was the decisive form of warfare. To Clausewitz, defense engendered passivity on the part of the defender and did achieve decisive victory. His concept of warfare saw defense as a "shield of blows" utilized to husband resources for the opportune moment to launch the counterattack.[128]

Similarly, a strategy of deterrence overly reliant on defense may also be inadequate. Information systems have limited resiliency to counter a successive series of IW attack. Countering blows to information systems and enduring successive IW attacks could eventually render an entire information system so corrupt that it is useless. It could also lead to a circumstance where backup systems can no longer restore key data and systems. In an age where threats spontaneously appear, adequately protecting the NII requires a defensive stance balanced with offensive actions.[129]

While each of these issues may shape future debates on how the US should protect the NII, they should not detract from the central focus the DoD should play in large role in NII protection. The DoD is well positioned to contribute a plethora of expertise, resources, and manpower toward protecting the NII. With vast experience in protecting vital national interests, the DoD's prime role of defending the MEII is one it is well suited for. While current structures and policies may require changes with in the nation's premier defense organization, no match in either the government or civil sector can compare to its abilities to protect the MEII. As the debate continues to take shape in years to come, it should always keep the DoD as the cornerstone protector of critical information infrastructures the US will most certainly become more reliant upon in the future.

Endnotes

[1] Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Pub 3-13.1 Joint Doctrine for Command and Control Warfare (C2W). Washington DC: U.S. Government Printing Office, 1996.

[2] "Joint Vision 2010" is the cornerstone for future joint warfighting operations. One of the foundational ideas illustrated in "Joint Vision 2010" is the necessity for information superiority in all future military operations spanning the spectrum of conflict. Information superiority is the dominating ability of information warfare to control information systems and ensure uninterrupted flow of information. Like air superiority, it can be local or general and does not connote full control over the entire information spectrum. To achieve the level of information superiority necessary for future operations requires unhindered access to the NII and DII and the assurance of integrity of the infrastructures. Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Vision 2010, Washington DC: U.S. Government Printing Office, p. 16; Tom Barrows, "Information Operations," *A Common Perspective*, March 1997, vol. 5 no.1, p. 13

[3] The physical evidence of widespread, coordinated information attack on the US vital NII is anecdotal and confined to postulation and exercises. Most of the attacks to date have been either perpetrated by personnel inside an organization or by curious and malicious hackers bent on breaking into systems for the challenge it presents. However, simulations and exercises, such as ELIGIBLE RECIEVER 1997 and the Rand Corporation "The Day After... in Cyberspace" study, demonstrate the increasing impact well timed and coordinated assaults on the NII and DII and the chaos they can create. The real vulnerability of the NII is still largely a question for debate. Martin C. Libicki, Defending Cyberspace and Other Metaphors, (Washington DC: National Defense University Press, 1997) pp. 23-27.

[4] While the Rome Labs case represents a recent example of computer attack, the first widely publicized and perhaps most famous case involving unauthorized computer access via global computer networks is the case dubbed "The Cuckoo's Egg." For further reference to this case refer to Clifford Stoll's, The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. New York: Doubleday, 1989;

[5] This case received wide scale coverage in computer trade publications, The New York Times, and from computer hacker electronic magazines. The case also received high level review by the Senate Governmental Affairs Committee Permanent Investigations Subcommittee and the General Accounting Office. Along with other information, this case prompted former democratic Senator Sam Nunn to state, "Clearly the time think about the security of our information infrastructure is now. Just as we prepare for a conventional weapons attack, we must be ready for attacks on our computers." "Rome Labs, Air Force Command and Control Research Facility Penetration," [Document on-

line] (Crypt Newsletter 38, accessed on 5 Jan 1997); available from http://www.bogus.net/codex/ rome.html; Internet, p. 1

[6] Sniffer programs allow system administrator to legitimately diagnose computer systems for malfunctions and initiate repairs. The program is designed monitor the status of the system, highlight problem areas, and divulge passwords and access codes for system administrator use. Underground networks of computer hackers or criminals stockpile several sniffer programs for use. To use the sniffer program only requires it to be installed into the host machine by physical or electronic means. Winn Schwartau, Information Warfare: Chaos on the Electronic Superhighway. (New York: Thunder's Mouth Press, 1994), pp. 116-119

[7] Keystroke monitoring, similar to wire tapping, involves use software subroutines to capture all keystrokes used by an intruder during session when logged into a system. "Rome Labs," p. 6

[8] Phone phreaking is the illegal access to phone circuitry to place unauthorized phone calls, manipulate billing records, and use phone lines for generally illegal and unauthorized purposes. Ibid., p. 6

[9] Brock, pp. 13-14

[10] "Rome Labs, p. 2.

[11] David A. Fulghum, "Computer Combat Rules Frustrate the Pentagon," *Aviation Week and Space Technology*, Sept 15, 1997, p. 67

[12] Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, Cyberwar: Security, Strategy, and Conflict in the Information Age. (Fairfax: AFCEA International Press, 1996), pp. 20 & 92; Schwartau, p. 54; Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Pub 3-13.1 Joint Doctrine for Command and Control Warfare (C2W), Washington DC: U.S. Government Printing Office 1996, pp. I-2 & 3; Office of the Joint Chiefs of Staff Joint Electronic Library, Concept for Future Joint Operation, Expanding Joint Vision 2010, Washington DC: U.S. Government Printing Officer, May 1997, p. 84

[13] DODIIS is a worldwide computer network of forty nodes used to collect, process, store and disseminate electronic, photo, and human intelligence. Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Pub 2.01 Joint Intelligence Support to Military Operations. Washington DC: U.S. Government Printing Office, 1996, p. GL-6

[14] Joint Pub 3-13.1 Joint Doctrine for Command and Control Warfare (C2W), pp. I-1 & 2; Thomas G. Mahnken, "War in the Information Age," *Joint Force Quarterly*, Winter 1995-96, p. 40; Concept for Future Joint Operation, Expanding Joint Vision 2010, p. 39

[15] Joint Pub 3-13.1 Joint Doctrine for Command and Control Warfare (C2W), p. I-3; Campen, pp. 10, 23-26, 43, 165; Office of the Secretary of Defense, Information Warfare - Defense, Washington DC: U.S. Government Printing Office, 1996, pp. ES-3, 2-4, H-4 Planning Considerations for Defensive Information Warfare - Information Assurance, Washington DC, 1993, pp. 1-2

[16] Brock, p.

[17] Ibid., p. 6

[18] Dominate maneuver is the ability to position and effectively employ widely dispersed forces. Precision engagement is the ability locate and strike targets, and rapidly perform battle damage assessment. Full dimensional protection is the ability to control battle space and ensure freedom of action. Focused logistics seeks to fuse information with logistics and transportation technology to provide the ability to rapidly ship, track, and deliver vital sustainment. Full spectrum dominance combines all four operational concepts creates a future force dominating the entire spectrum of conflict. For a complete description of see Joint Vision 2010, pp. 20-27

[19] Ibid., pp. 2, 16-20

[20] Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Doctrine Encyclopedia (Draft), Washington DC: U.S. Government Printing Office, May 1997, p. 75

[21] A key element of C4IFTW is the Global Command and Control System (GCCS). GCCS gives commander's at all levels a fused picture of their battlespace enabling rapid and effective command, control, and communications of all forces. GCCS also incorporates key planning and assessment tools required by commanders to meet readiness requirements and deploy forces globally. For a survey of additional GCCS capabilities refer to Office of the Joint Chiefs of Staff Joint Electronic Library, CJCSM 3500.03 Joint Training Manual for the Armed Forces of the United States," Washington DC: U.S. Government Printing Office, p. annex A to Appendix L, Office of the Joint Chiefs of Staff Joint Electronic Library, User's Guide for JPOES (Joint Operation Planning and Execution system) Washington DC: U.S. Government Printing Office, and Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Pub 6-0, Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations Washington DC: U.S. Government Printing Office.

[22] Joint Pub 6-0, pp. II-11 to II-13; Joint Doctrine Encyclopedia (Draft), pp. 75-76, 309

[23] For additional information on civilian related computer attacks refer to Scott Charney, "Computer Crime" Department of Justice, Criminal Division, 1996, p. 6; George I. Seffers, "U.S. Readies Vaccine To Fight Virtual Virus," *Defense News*, (September 22-28, 1997) p. 1 & 60; Office of the Secretary of Defense, Information Warfare - Defense. Washington DC: U.S. Government Printing Office, 1996, p. 2-15; Brock, p. 4

[24] Brock, p. 13.

[25] Ibid., pp. 19-20

[26] Schwartau, pp. 215-248

[27] Libicki, p. 14

[28] Gateways are nodes into computer systems. When comprised as general purpose computers, they embody all of the typical vulnerabilities of stand alone or remotely connected computers possess. Terminal servers Routers are hardware devices generally designed to control network traffic and prevent network overloading areas with large network environments.

[29] Robert T. Marsh, Critical Foundations: The Report of the President's Commission on Critical Infrastructure Protection, (White House: Washington DC: Oct 1997), p. 9; Planning Considerations for Defensive Information Warfare - Information Assurance, pp. 11-12, 36-37.

[30] Software attack methods increase daily. Intruders attack information systems using a variety of methods including E-mail bombs, logic bombs, pinging, computer hijacking, and viruses. E-mail bombing involves sending millions of E-mail messages intent on overloading phone services and crashing networks. Logic bombs are programs activated by key words or phrases with the intent of causing harm to computer systems. An example of a logic bomb would be the activation of a program designed to erase a computer hard drive when the user types in the phrase "Mickey mouse." Pinging involves deliberately sending a ping or packet of data larger than 65,536 bytes to a remote machine. Depending upon the computers operation system, the result of pinging could be to crash, reboot, or kill a significant number of systems. Computer hijacking involves intruders stealing passwords and taking over systems such as air traffic control. Viruses are segments of software written to implant themselves into key operating system files and adversely affect the host computers operation. They are typically designed to infect system unknowingly and can be either benign or malignant. Marsh; Schwartau, p. 104; "Symantec Antivirus Research Center."

[31] One example of the how an unintentional software error caused serious malfunctions of the telecommunications network occurred in 1991 when a major failure of several telephone switches in several large cities resulted from a three bit error in a single byte of a scheduled software upgrade. Planning Considerations for Defensive Information Warfare - Information Assurance, pp. 36-37; Campen, p.94

[32] Systems designed with open architecture seek to make access from public networks and network services from any number of network and non-network related service providers readily available, Information Warfare-Defense, p. 2-10

[33] A "back door" is a file inserted into a computers operating system designed to circumvent existing security measures.

[34] U.S. Army, FM 100-5 Operations, Washington DC: U.S. Government Printing Office, 1993, p. 6-7.

[35] Schwartau, p. 52;

[36] Warden, John A., The Air Campaign, (Washington DC: National Defense University Press, 1988). P. 9. Col John Warden, USAF (ret.), is a modern day airpower theorist and originator of many of the strategic concepts surrounding the air campaign undertaken during Desert Storm. His writing includes "The Air Campaign" and many companion articles. Studying Warden's system of systems approach reveals many of the theoretical underpinnings of current Air Force doctrine and serves as a useful tool to manipulate and apply. While analyzing Air Force doctrine may demonstrate application of his theory's, some of Warden's theoretical constructs useful to this discussion were altered or omitted.

[37] Warden's five centers of gravity include leadership, organic essentials, infrastructure, population, and fielded forces are arranged concentrically with leadership residing in the inner ring and fielded forces residing on the outer ring. Under Warden's concept, leadership represents the most important of all the rings and should be the focus of military campaigns. For a complete synopsis of Warden's concepts see Phillip S. Meilnger, The Paths of Heaven: The Evolution of Airpower Theory, (Maxwell Air Force Base, Montgomery Alabama: Air University Press, 1997) pp. 371-384

[38] Ibid., pp. 371-373.

[39] Joint Pub 3.0 Doctrine for Joint Operations, pp. III-20 and III-21

[40] James R. Beniger, The Control Revolution, (Cambridge: Harvard University Press, 1986) pp. 1-60.

[41] Campden, pp. 197-198

[42] For a complete description of operational art and its emergence see Schneider, James J., "The Theory of Operational Art", Theoretical Paper No. 3, School of Advanced Military Studies, Ft Leavenworth, 1 March 1988.

[43] James J. Schnieder, *Black Lights: Chaos, Complexity, and the Promise of Information Warfare. Joint Force Quarterly* (Spring 97) pp. 27

[44] Alvin Toffler and Heidi Toffler. War and Anti-War: Survival at the Dawn of the 21st Century. (Boston: Little, Brown, and Company, 1993) pp. 69-79

[45] Ibid., pp. 57-63

[46] Libicki, pp. 11-12; "President's Commission on Critical Infrastructure Protection," [Document on-line] (Washington DC: The White House, 1996, accessed on 26 Oct 1997); available from http://www.info-sec.com/pccip/web; Internet, pp. 3-10

[47] FM 100-5 Operations, p. Glossary-2

[48] Joint Pub 3.0 Doctrine for Joint Operations, pp. III-21 & III-22

[49] Kennedy, Kevin J., Bruce M. Lawlor, Arne J. Nelson, "Grand Strategy for Information Age National Security," Policy Analysis Paper, (Cambridge: John F. Kennedy School of Government), p. 6-7

[50] Office of the Secretary of Defense, Information Warfare - Defense, (Washington DC: U.S. Government Printing Office, 1996), pp. 4-1 & 4-2; "National Security Strategy A National Security Strategy for A New Century," [Document on-line] (Washington DC: The White House, May 1997, accessed on 17 Jan 1998); available from National Security Council http://www.whitehouse.gov/WH/EOP/ NSC/Strategy, Internet; "President's Commission on Critical Infrastructure Protection," pp. 3-6.

[51] Information Warfare - Defense, pp. 6-22 & 6-23

[52] "National Security Strategy A National Security Strategy for A New Century," [Document on-line] (Washington DC: The White House, May 1997, accessed on 17 Jan 1998); available from National Security Council http://www.whitehouse.gov/WH/EOP/ NSC/Strategy; Internet.

[53] Information Warfare - Defense, pp. ES-2 to ES-3, 4-1 to 4-2.

[54] Information Warfare - Defense, p. 2-1; Planning Considerations for Defensive Information Warfare - Information Assurance, pp. 1-2

[55] Planning Considerations for Defensive Information Warfare - Information Assurance, p ES-1.

[56] Popularized by Alvin and Heidi Toffler, the "Third Wave" represents a fundamental shift in a nations foundational economic and military strengths. The Toffler's contend that three waves have characterized human development. In the "First Wave" society was primarily agrarian and warfare revolved around conquering territory. In the "Second

Wave" society shifted to industrial production methods and industrial warfare based on attrition. In the "Third Wave" society is dominated by its ability to perform information functions and warfare targets these information based functions to damage or destroy the societal foundations. Toffler, pp. 9-80

[57] For a complete discussion pertaining to specific contents of a national information policy see Winn Schwartau, Information Warfare: Chaos on the Electronic Superhighway, New York: Thunder's Mouth Press, 1994; Campden., p 248; Schwartau, pp. 316-342

[58] Laissez faire information infrastructure protection builds on the notion that current mechanisms exist to counter system wide vulnerabilities. As the vulnerabilities grow and evolve so to will the defense mechanisms. The prime motivating factor is this strategy is economic motivation driving technological innovation and defense. In the "seize the initiative approach," federal authorities develop proactive plans to manage and protect the information infrastructure. Round, p. 4.

[59] While information superiority represents a worthwhile goal, some experts and theorists it is an unachievable benchmark. Rapidly changing technology, new innovation in information transfer, and the inability for any single entity to keep pace with changing technology represent arguments against attaining information superiority. Some experts it is better to strive for information parity vice information superiority so as not to waste financial and human resources on trying to attain the unattainable.

[60] Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Vision 2010, Washington DC: U.S. Government Printing Office, p. 16; Tom Barrows, "Information Operations," *A Common Perspective*, March 1997, vol. 5 no.1, p. 13

[61] The model proposed for the shift of broad based manufacturing to narrow based information dominance does not imply previous manufacturing based society was not interconnected. Rather, it implies a manufacturing based economy is not dependent on single nodes to generate economic or military power. Conversely, information based economies and militaries tend to be more singularly reliant upon information for all functions. Information Warfare - Defense, p. 2-3

[62] Libicki, p. 18

[63] Campden, pp. 95-96

[64] "President's Commission on Critical Infrastructure Protection," p. 48; Information Warfare - Defense, p. ES-4 and ES-5

[65] Schwartau, pp. 316-353

[66] "President's Commission on Critical Infrastructure Protection," p. 48; Information Warfare - Defense, p. ES-4 and ES-5

[67] In this instance local refers to the theater of operations geographically delineated as southwest Asia. The region nations on the Arabian Peninsula, and Turkey, Syria, Jordan, Israel, and Egypt.

[68] The US Armed Forces utilized a series of communications links and remote sensing locations to track theater ballistic missile launches in the area of responsibility. The links provided real time alerts to theater forces and aided in cueing defensive measures to counter incoming missiles.

[69] Kennedy, Kevin J., Bruce M. Lawlor, Arne J. Nelson, "Grand Strategy for Information Age National Security," Policy Analysis Paper, (Cambridge: John F. Kennedy School of Government), pp. 3-1 to 3-3

[70] Toffler, p. 141-142, Campden, pp. 170, 201.

[71] E-mail bombing involves sending millions of E-mail messages intent on overloading phone services and crashing networks. Logic bombs are programs activated by key words or phrases with the intent of causing harm to computer systems. An example of a logic bomb would be the activation of a program designed to erase a computer hard drive when the user types in the phrase "Mickey mouse." Pinging involves deliberately sending a ping or packet of data larger than 65,536 bytes to a remote machine. Depending upon the computers operation system, the result of pinging could be to crash, reboot, or kill a significant number of systems. Computer hijacking involves intruders stealing passwords and taking over systems such as air traffic control. Viruses are segments of software written to implant themselves into key operating system files and adversely affect the host computers operation. They are typically designed to infect system unknowingly and can be either benign or malignant. "Presidents Commission on Critical Infrastructure Protection"; Schwartau, p. 104; "Symantec Antivirus Research Center."

[72] Blake Harris, "Advent of Information Warfare," [Internet Document] http:www.i-war.com/advent.htm, p. 1-3; "Information Warfare - Defense," p. 2-1

[73] Kennedy, Lawlor, and Nelson, pp. 3-5 to 3-7.

[74] Report of the National Defense Panel, Transforming Defense, National Security in the 21st Century, Washington DC, 1997, p. 13

[75] Martin Van Crevald, Command in War. Cambridge: Harvard University Press, 1985, pp. 264-268. Van Crevald in his book illustrates that a common thread running through several conflicts is that advanced information processing capabilities does not increase certainty in decision making. His case studies of the 1973 Arab-Israeli War, the US experience in Vietnam, and other conflicts points toward the futility of trying to increase decision making certainty with technology.

[76] Transforming Defense, National Security in the 21st Century, p. 10; Rosecrance, Richard. "The Rise of the Virtual State." Foreign Affairs (July/August 1996) pp. 45-61; Matthews, Jessica T., "Power Shift." Foreign Affairs (January/February, 1997) pp. 50-66

[77] Campden, p. 274. An interesting situation occurs with the link between the NII and DII. While a symbiotic relationship exists between both systems, the majority of the components are either owned or operated by civilian/commercial organizations. For example, much of the DII telecommunications network travels over commercial segments of the public switch network. Furthermore, much of the personal computer inventory and integrated circuit components found within the DoD are the result of Commercial Of the Shelf (COTS) program initiatives.

[78] "Oath of Office" all miltary Officers' and Noncommisioned Officers' must recite upon entering active duty, undergoing promotion, or re-enlistment. Full text of the oath is cited below. "I, FULL NAME, do solemnly swear (or affirm) that I will support and defend the Constitution of the United States against all enemies, foreign and domestic, that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion, and that I will well and faithfully discharge the duties of the office upon which I am about to enter. SO HELP ME GOD." [Document on-line] accessed on 8 Mar 1998); available from http://www.usc.edu/dept/afrotc/cadets/warrior/oath.html, Internet

[79] Transforming Defense, National Security in the 21st Century, p. 2-28

[80] Campden, p. 94

[81] Kennedy, Lawlor, Nelson, p. 3-14.

[82] "President's Commission on Critical Infrastructure Protection," p. 27-35

[83] Campden, p. 270-271

[84] William J. Gregor, "Toward a Revolution in Civil -Military Affairs, Understanding the United States Military in the Post Cold War World," Working Paper No. 6, (Cambridge: John M. Olin Institute for Strategic Studies, August 1996), p. 1 Dr. Gregor argues in his paper that while it may appear an affront to both military and non-military personal, the military has always shared in making United States foreign policy. Whether during the deliberate or crises action planning process or when actually assigned the roles by past Presidents the military has in some form been inextricably interwoven into the policy determination environment of the US political system.

[85] Kennedy, Lawlor, and Nelson, pp. 6-3 and 6-4.

[86] The national intelligence agencies refers to those organizations providing intelligence information supporting national security efforts. Generally they include the Central Intelligence Agency and the National Security Agency.

[87] Fulghum, David A., "Cyberwar Plans Trigger Intelligence Controversy," Aviation Week and Space Technology (Jan 19, 1997), p. 52. The controversy outlined is nothing new. Stovepipe national intelligence systems prevented warfighters at the beginning of Desert Storm from possessing up to date intelligence photos. Due to security classifications and compartmentalization of information, some national reconnaissance information was not available to front line combat forces.

[88] Kennedy, Lawlor, and Nelson, pp. 6-5 and 6-6.

[89] Toffler, p. 141-142, Campden, pp. 170, 201

[90] Campden, p. 80

[91] Ibid., p. 79-80

[92] Conceptually limiting the protection of cyberspace to only critical systems inherently contains two assumptions. First, it assumes the number of critical infrastructures remains within a certain limited growth rate. Second, it assumes that private owners of NII components will take steps to secure critical systems. Libicki, pp. 32-33

[93] Analyzing IW attacks reveals many of the vulnerabilities existing in today's information systems and information infrastructure relate to human factors, drives toward open architecture and interconnection of civilian and military networks. Human factors contribute to a large majority of the vulnerabilities. Poor password protection, physical security, and lack of vigilance by system administrators allow IW attackers to install "back doors" and steal, alter, and destroy critical information.

[94] President's Commission on Critical Infrastructure Protection, pp. 27-66; Transforming Defense, National Security in the 21st Century, pp. 25-28.

[95] Drives toward designing open network architecture increases the vulnerability of intruders attacking the information system. Protocol-based weaknesses in authentication and cryptosystem weaknesses involving inadequate key size demonstrate further information system vulnerabilities. Systems designed with open architecture seek to make access from public networks and network services from any number of network and non-network related service providers readily available, "Information Warfare-Defense," p. 2-10

[96] Information Warfare - Defense, p. 2-7 to 2-9.

[97] While setting industry standards for fault tolerant computing hardware and software seems an easy solution, many nuances currently prevent such solutions. Legislation enacting such standards, such as the "Clipper Chip," raises deep concerns from both civil libertarians and industry groups alike. Furthermore, enforceability of such standards in a global manufacturing environment also clouds the issue.

[98] Campen, p. 86

[99] An example of the legal problems in criminalizing computer crime is found by examining the Computer Fraud and Abuse Act (CFAA). CFAA made theft of computer resources a criminal act. However, several problems exist currently with the act. First, the act focuses on method of entry into a computer system versus how the computer system was used thus possibly excluding wide bodies of potentially criminal acts. Second, the fraud provision of the CFAA prohibits prosecution of unauthorized information system use if the object obtained only consists of the use of a computer." Office of the Joint Chiefs of Staff, Information Warfare Division (J6K), Command, Control, Communications, and Computer Directorate, Information Warfare, Legal, Regulatory, Policy, and Organizational Considerations for Assurance. Washington DC: Science Applications International Corporation (SAIC), July 1995, p. 2-25.

[100] Ibid., pp. 2-16 to 2-20.

[101] The complexity of the organizational environment is best illustrated by examining the various stakeholders in the NII and DII protection process. They include national, federal, and state/local interests as well as private industry, academia, and public interest groups. Each group represents conflicting goals, interests and priorities. For example, the defense interests primarily lie in protecting the nation from threats while private industry primarily are concerned with protecting the NII to further economic interests. Information Warfare, Legal, Regulatory, Policy, and Organizational Considerations for Assurance, pp. 2-13 to 2-71, 3-1 to 3-6

[102] None of the discussion about organizational or legal complexities of current structures included any reference to regulatory or policy requirements. Adding these two area only adds further complexity to the situation. Ibid., pp. 2-17 to 2-50

[103] Ibid., p. 2-53.

[104] Laws of war are the basis for rules of engagement. Within the context of warfare, laws, rules and regulations exist to regulate violence. They exist because of the uncertainty of warfare and because the degradation and chaos that exists on the battlefield and the road of total irrationality down which it can lead combat forces. Laws of war also aim at defining the limits of violence. For the combatants to know who and what they can target, the reason they are targeting them, and the lengths and methods they are allowed to utilize to strike those targets requires carefully defining the limits of violence. In a modern context, ROE serve as the legal manifestation of laws of war. Martin van

Crevald, Martin. The Transformation of War, (New York: The Free Press, 1991), pp. 87-94

[105] In this instance, national intelligence agencies refers to a single cooperative body of intelligence organization. Generally, this scheme would combine the CIA, NSA, DIA, and other national level intelligence organizations into one body.

[106] President's Commission on Critical Infrastructure Protection, pp. 27-46.

[107] Ibid., pp. 29-46.

[108] Campden, pp. 80-84, 103

[109] The need to classify sensitive techniques and information sources will continually require national intelligence agencies maintain a modicum of secrecy within their operations. However, in an information age, there is growing requirement for sensitive information distribution to non-traditional users. The point to recognize is the continual debate over offense versus defense in the intelligence community. Intelligence officials argue to publicize information could potentially damage future ability to roam freely among key networks to clandestinely gather information. Conversely, offensive minded personnel, particularly in the DoD argue information gathering must also be accompanied by action.

[110] Campen, pp. 80, 84, 269; "Cyberwar Plans Trigger Intelligence Controversy," pp. 52-54; "President's Commission on Critical Infrastructure Protection," pp. 27-31.

[111] Transforming Defense, National Security in the 21st Century, p. 27

[112] Campden, p. 101

[113] Kennedy, p. 7-4

[114] Care should be taken not to confuse lead agent or "significant role" as sole protector. The intent of the DoD as lead agent in this sense is to serve as a facilitator versus a commander. "President's Commission on Critical Infrastructure Protection," pp. 54-55.

[115] Transforming Defense, National Security in the 21st Century, p. 27

[116] "Executive Order no. 12656, Assignment of Emergency Preparedness Responsibilities," 53 Federal Register 226, 18 Nov 1988; Executive Order no. 12919, National Defense Industrial Resources Preparedness, 59 Federal Register 29525, 3 Jun 1994; Executive Order no. 12148, Federal Emergency Management," 44 Federal Register 43239, 20 July 1979; Executive Order no. 12472, Assignment of National Security and

Emergency Preparedness Telecommunications Functions," 49 Federal Register 13471, 3Apr. 1984.

[117] Kennedy, p. 6-3 to 6-4

[118] While theoretically market forces and what Adam Smith, a well known 18th century English economist, labeled the invisible hand will respond to such threats the problem lies in defining "trivial" security problems. Defining "trivial" security problems entails identifying thresholds or criteria across a broad spectrum of diverse information uses. For example, inability to access a local Internet service provider for 15 minutes may be a minor annoyance to an individual while the same denial of service to a regional brokerage firm could represents millions of dollars in lost revenue.

[119] For example, every new computer virus introduced produces a myriad of responses from commercial companies protecting against its effects.

[120] Cascading effects entails the propagation of failures to a wide span of systems from a failure at a single node or a set of critical nodes. While possible it requires close coordination and numerous assets. Libicki, p. 27, Round, Oscar W., "Defining Civil Defense in the Information Age," [Document on-line] (Strategic Forum Number 46, September 1995, accessed on 15 Dec 1997); available from http://www.ndu.edu/ndu/inss/strforum/forum46.htm, p. 4

[121] Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Pub 3.0 Doctrine for Joint Operations, Washington DC: U.S. Government Printing Office, 1996, p. III-4.

[122] Information Warfare, Legal, Regulatory, Policy, and Organizational Considerations for Assurance, pp. 2-13 to 2-71

[123] Kennedy, pp. 6-9 and 6-10;

[124] An isolation routine is a set of software instructions designed to isolate a given information system from its outside links. The routine can be likened to building walls around a system not permitting it to interact with outside environments. This concept can be further extended to nations. Isolation routines could be enabled preventing nations from utilizing many of the electronic media from interacting on the GII. Campden, p, 243-248

[125] Libicki, p. 42

[126] It is highly dubious to think information attackers will be easily tracked and linked to their actions. Perpetrators of IW usually do not leave trademarks, fingerprints, or signatures. They typically rely on stealth and speed to break in to information systems. Furthermore, any entity carefully planning a coordinate IW attack would probably not leave a signature or calling card linking them back to the crime. Libicki, p. 49.

[127] In this instance the problem relates to developing criteria governing the level of retaliatory response. "Defining an actionable incident means determining how much harm is enough." Libicki, p. 41-54

[128] Carl von Clausewitz, On War. Princeton: Princeton University Press, 1976, pp. 357-392

[129] Campden, p. 80

Bibliography

Books

Allard, C. Kenneth. Command, Control, and the Common Defense. New Haven: Yale University Press, 1990.

Beniger, James R. The Control Revolution, Cambridge: Harvard University Press, 1986.

Campen, Alan D., Douglas H. Dearth, and R. Thomas Goodden. Cyberwar: Security, Strategy, and Conflict in the Information Age. Fairfax: AFCEA International Press, 1996.

Clausewitz, Carl Von, On War. Princeton: Princeton University Press, 1976.

De Landa, Manuel. War in the age of Intelligent Machines. New York: Zone Books, 1991.

Libicki, Martin C., Defending Cyberspace and Other Metaphors, Washington DC: National Defense University Press, 1997.

Meilnger Phillip S., The Paths of Heaven: The Evolution of Airpower Theory. Maxwell Air Force Base, Montgomery Alabama: Air University Press, 1997.

Quittner, Joshua and Michele Slatalla. Masters of Deception, the Gang that Ruled Cyberspace. New York: Harper Collins, 1995.

Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway. New York: Thunder's Mouth Press, 1994.

Snyder, Frank M. Command and Control: The Literature and Commentaries. Cambridge: Harvard University, 1989.

Stoll, Clifford. The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. New York: Doubleday, 1989.

Toffler, Alvin and Heidi Toffler. War and Anti-War: Survival at the Dawn of the 21st Century. Boston: Little, Brown, and Company, 1993.

van Crevald, Martin. The transformation of War. New York: The Free Press, 1991.

_____. Command in War. Cambridge: Harvard University Press, 1985.

Warden, John A. III. The Air Campaign: Winning for Combat. Washington DC: NDU Press, 1988.

Articles

Barrows, Tom. "Information Operations." A Common Perspective, (March 1997, vol 5 no.1).

Boorda, Jeremy M. "Leading the Revolution in C4I." Joint Force Quarterly (Autumn 1995)

Burton, Daniel F., "The Brave New Wired World." Foreign Policy (Spring 1997) pp. 23-38

Fulghum, David A., "Computer Combat Rules Frustrate the Pentagon." Aviation Week and Space Technology (Sept 15, 1997)

_____. "Cyberwar Plans Trigger Intelligence Controversy," Aviation Week and Space Technology (Jan 19, 1997)

Gumahad, Arsenio T., "The Profession of Arms in the Information Age." Joint Force Quarterly, (Spring 97) p.19

Kraus, George F. "Information Warfare in 2015." U.S. Naval Institute Proceedings (August 1995), pp. 42-45

Mahnken, Thomas G., "War in the Information Age." Joint Force Quarterly (Winter 1995-96) p. 42

Mathews, Jessica T., "Power Shift." Foreign Affairs (January/February, 1997) pp. 50-66

Nye, Joseph, William Owens, and Eliot Cohen. "The Information Edge." Foreign Affairs (March/April 1996) pp. 20-36

Rosecrance, Richard. "The Rise of the Virtual State." Foreign Affairs (July/August 1996) pp. 45-61

Ryan, Donald E., "Implications of Information-Based Warfare." Joint Force Quarterly (Autumn-Winter 94-95) pp. 114-116.

Schnieder, James, J., "Black Lights: Chaos, Complexity, and the Promise of Information Warfare." Joint Force Quarterly (Spring 97) pp. 21-28

____, "The Theory of Operational Art", Theoretical Paper No. 3, School of Advanced Military Studies, Ft Leavenworth, 1 March 1988. pp. 1-53

Seffers, George I., "U.S. Readies Vaccine To Fight Virtual Virus." Defense News. (September 22-28, 1997) pp. 1 & 60

Struble, Dan. "What is command and control warfare?" Naval War College Review, (Summer 95) pp. 89-98.

Government Documents

Office of the Joint Chiefs of Staff Joint Electronic Library, CJCSM 3500.03 Joint Training Manual for the Armed Forces of the United States. Washington DC: U.S. Government Printing Office, May 1996.

Office of the Joint Chiefs of Staff Joint Electronic Library, Command, Control, Communications, and Computer Directorate, Information Warfare, Legal, Regulatory, Policy, and Organizational Considerations for Assurance. Washington DC: Science Applications International Corporation (SAIC), July 1995.

Office of the Joint Chiefs of Staff Joint Electronic Library, Concept for Future Joint Operation, Expanding Joint Vision 2010. Washington DC: U.S. Government Printing Officer, May 1997.

Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Doctrine Encyclopedia (Draft). Washington DC: U.S. Government Printing Office, May 1997.

Office of the Joint Chiefs of Staff Joint Electronic Library, JCS Memo of Policy (MOP) 30, Command and Control Warfare. Washington DC: U.S. Government Printing Office, 1993.

Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Vision 2010. Washington DC: U.S. Government Printing Office, May 1997.

Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Pub 1.0 Joint Doctrine for Command and Control Warfare (C2W). Washington DC: U.S. Government Printing Office, 1996.

Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Pub 2.01 Joint Intelligence Support to Military Operations. Washington DC: U.S. Government Printing Office, 1996.

Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Pub 3.0 Doctrine for Joint Operations. Washington DC: U.S. Government Printing Office, 1996.

Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Pub 3-13.1 Joint Doctrine for Command and Control Warfare (C2W). Washington DC: U.S. Government Printing Office, 1996.

Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Pub 6-0, Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations Washington DC: U.S. Government Printing Office.

Office of the Joint Chiefs of Staff Joint Electronic Library, User's Guide for JOPES (Joint Operation Planning and Execution system) Washington DC: U.S. Government Printing Office

Office of the Secretary of Defense, Information Warfare - Defense. Washington DC: U.S. Government Printing Office, 1996.

Science Applications International Corporation. Planning Considerations for Defensive Information Warfare - Information Assurance. Washington DC, 1993.

Report of the National Defense Panel, Transforming Defense, National Security in the 21st Century, Washington DC, 1997

School of Advanced Military Studies

Schneider, Michael W., Electromagnetic Spectrum Domination: 21st Century Center of Gravity or Achilles Heel? SAMS Monograph, Fort Leavenworth, 1994.

Smith, Kevin B., The Crises and Opportunity of Information War. SAMS Monograph, Fort Leavenworth, 1994.

Theses, Studies, and Other Papers

Bond, James N., Peacetime Foreign Date Manipulation As One Aspect of Offensive Information Warfare: Questions of Legality under the United Nations Charter Article 2(4). 1996.

Charney, Scott. Computer Crime. Department of Justice, Criminal Division, 1996.

Gregor, William J., "Toward a Revolution in Civil -Military Affairs, Understanding the United States Military in the Post Cold War World", Working Paper No. 6, (Cambridge: John M. Olin Institute for Strategic Studies, August 1996)

Information Warfare and the Use of Force Among Nations, No author and no date apparently written as background information for ROE development officials on USAF Staff.

Kennedy, Kevin J., Bruce M. Lawlor, Arne J. Nelson, "Grand Strategy for Information Age National Security," Policy Analysis Paper, (Cambridge: John F. Kennedy School of Government)

Krepinevich, Andrew F., Keeping Pave with the Military-Technological Revolution. Military Technology, 1994.

E-Mail and Other Electronic Documents

Brock, Jack L., "GAO Executive Report B-266140." [Document on-line] Washington DC: accessed Oct 1996); available from http://www.infowar.com/civil_de/gaosum.html-ssi; Internet

"National Security Strategy A National Security Strategy for A New Century," [Document on-line] (Washington DC: The White House, May 1997, accessed on 17 Jan 1998); available from National Security Council http://www.whitehouse.gov/WH/EOP/ NSC/Strategy; Internet

"President's Commission on Critical Infrastructure Protection," [Document on-line] (Washington DC: The White House, 1996, accessed on 26 Oct 1997); available from http://www.info-sec.com/pccip/web; Internet.

Round, Oscar W., "Defining Civil Defense in the Information Age." [Document on-line] (Strategic Forum Number 46, September 1995, accessed on 15 Dec 1997); available from http:// www.ndu.edu/ndu/inss/strforum/forum46.htm; Internet

"Rome Labs, Air Force Command and Control Research Facility Penetration," [Document on-line] (Crypt Newsletter 38, accessed on 5 Jan 1997); available from http://www.bogus.net/codex/ rome.html; Internet

"Symantec Antivirus Research Center," [Document on-line] (Symnatec Corporation, 1996/1997, accessed on 26 Oct 1997); available from http://www.symantec.com/avcenter/vinfodb.html; Internet.